现代数学丛书

冯克勤 著

分圆函数域

CYCLOTOMIC FUNCTION FIELDS

FENG KEQIN

上海科学技术出版社

·现代数学丛书·

分圆函数域

冯克勤 著

上海科学技术出版社

责任编辑　赵序明

·现代数学丛书·
分 圆 函 数 域
冯克勤　著
上海科学技术出版社出版、发行
（上海瑞金二路 450 号）
新华书店上海发行所经销　　上海商务印刷厂印刷
开本 787×1092　小 1/16　印张 14.25　插页 4　字数 182 000
1997 年 7 月第 1 版　1997 年 7 月第 1 次印刷
印数 1—1 200
ISBN 7-5323-3949-1/O·200
定价：30.00 元

内 容 提 要

本书系统介绍近20年来发展的分圆函数域理论．整理了Carlitz、冯克勤、Gekeler、D. Goss、D. Hayes、M. Rosen和Thakur等学者在这一领域的研究成果．主要内容有：分圆函数域的基本性质、分圆单位、欧拉系、类数整除性和函数域上的分析学(Mahler定理的模拟、P-adic Gamma函数、高斯和、分布与测度)．本书也可看作是进一步理解一般函数域上的Carlitz模理论和Drinfeld模理论的入门书．

本书供数学研究工作者；高等学校数学专业的教师、研究生、高年级学生学习参考．

Modern Mathematics Series

CYCLOTOMIC FUNCTION FIELDS

Feng Keqin

Shanghai Scientific & Technical Publishers

Cyclotomic function fields

Feng Keqin

Abstract

The purpose of this book is to introduce the cyclotomic function field theory developmented in last two decades, and to collected systematically the research contributions of Carlitz, Keqin Feng, Gekeler, D. Goss, D. Hayes, M. Rosen, Thakur etc. in this branch of number theory. The main contents are: basic properties of cyclotomic function fields, cyclotomic units, Euler system, divisibility of class numbers and analysis on function fields (analogy of the Mahler's theorem, P-adic Gamma function, Gauss sum, distribution and measure). The book can also be viewed as an introduction for further understanding of the Carlitz module theory on general function fields and the Drinfeld module theory.

出版说明

从60年代起，由华罗庚教授任主编的《现代数学丛书》编辑委员会曾组织编著，并由我社出版了多部具有很高水平的数学学术专著，有几部专著并已在国外出了外文版，受到国内外数学界和广大读者的高度重视，获得了很高的评价。原编委会中华罗庚、关肇直、吴新谋三位教授虽已先后逝世，但他们为本《丛书》所作出的贡献迄今仍为人们所敬仰、怀念。由于某些客观原因，《现代数学丛书》的出版工作曾一度停顿。

为了适应现代数学的迅速发展，更好地反映我国数学家近几年的优秀研究成果，必须大力加强《现代数学丛书》的规划、编辑、出版工作，充实编委会的力量。考虑到不少编委年事已高，经向原编委会中大部分同志及数学界有关专家广泛征求意见后，于1990年对编委会作了调整，补充了一些著名的中年数学家和学科带头人，建立了新的编委会，并进一步明确了本丛书的宗旨。

《现代数学丛书》新的编辑委员会由苏步青教授任名誉主编、谷超豪教授任主编，18位著名数学家任委员。编委会负责推荐(或审定)选题和作者，主持书稿的审核等工作。

《现代数学丛书》的宗旨是：向国内外介绍我国比较成熟的、对学科发展方向有引导作用的、国内第一流水平的数学研究成果，反映我国数学研究的特色和优势，扩大我国数学研究成果的影响，促进学科的发展和国内外的学术交流。

为了实现上述宗旨，本丛书将陆续组织出版在基础数学、应用数学和计算数学方面处于学科发展前沿、有创见且具有系统完整

研究成果的现代数学学术专著。

为出版好《现代数学丛书》，我们热切地期望着数学界各位专家的大力支持和悉心指导，并欢迎广大读者提出宝贵的建议和意见。

上海科学技术出版社

前　言

数域的研究起源于数论(不定方程的整数解),单变量函数域的研究起源于几何(代数曲线)。在本世纪初,Hensel 建立了赋值理论之后,这两种域的研究形成了统一的手段(整体域理论)。经典代数数论和代数曲线算术理论相交织,成为现代算术代数几何的一个源头。

如果特别地看一下分圆理论发展的历史,更可体会到数域和函数域相互启发和促进的生动情景。经典的分圆数域理论是在上世纪后半叶由 Kummer 和 Hilbert 给出的。近代分圆数域理论的标志之一是 Iwasawa 于 1959 年给出的分圆 $\boldsymbol{Z}_p$ 扩张以及一般 $\boldsymbol{Z}_p$ 扩张的类数公式。这个公式的建立受到了(有限域上单变量)函数域的 Weil 定理的启发:数域的 $\boldsymbol{Z}_p$ 扩张类比于函数域的常数域无限扩张。不过,前者比后者复杂,内容也更加丰富和深刻,这方面可见 Washington[57]或 Lang S[45]的书。对于许多数论问题,函数域情形比数域情形容易解决,其中一个重要的原因是:函数域上有 Weil 定理。而对于数域情形,相应的黎曼猜想没有解决。但是情况也不完全如此。例如说,早在上世纪末就证明了:有理数域 $\boldsymbol{Q}$ 的最大阿贝尔扩域是所有分圆数域 $\boldsymbol{Q}(\zeta_n)$ 的合成 $\left(\zeta_n=e^{\frac{2\pi i}{n}},n\geqslant 3\right)$ (Kronecker-Weber 定理). 对于函数域,类似的问题是:对于有限域 $\boldsymbol{F}_q$ 上的有理函数域 $k=\boldsymbol{F}_q(T)$,如何具体构作出 k 的最大阿贝尔扩域? 这个问题一直到 1974 年才由 Hayes D[39]解决. 在 30 年代,Carlitz 和他的一些学生对于一些古典的

数论问题，研究了在有理函数域$k=\boldsymbol{F}_q(T)$和多项式环$R=\boldsymbol{F}_q[T]$上的类似问题（k 和 R 分别是 $\boldsymbol{Q}$ 和整数环 $\boldsymbol{Z}$ 的类比）. 特别是，Carlitz 构作出 k 的一类有限阿贝尔扩域。我们可以把上述 Kronecker-Weber定理说成为：$\boldsymbol{Q}$ 的最大阿贝尔扩域是将 $\boldsymbol{Q}^{ac}$（$\boldsymbol{Q}$ 的代数闭包）的乘法群（作为 $\boldsymbol{Z}$-模）的所有 torsion 点（有限阶元素，即单位根）添加到 $\boldsymbol{Q}$ 上而得到的域。Carlitz 的主要贡献是：他给出了 k^{ac}（$k=\boldsymbol{F}_q(T)$的代数闭包）的一种特别的 R-模结构（现在被人们称之为Carlitz 模），并且证明了对于这种 R-模 k^{ac} 的每个 torsion 元素 λ，$k(\lambda)/k$都是（有限）阿贝尔扩张。到了 1974 年，Hayes 利用类域论证明了：Carlitz 给出的所有扩域 $k(\lambda)$以及 k 的所有常数域扩张的合成就是 k 的最大阿贝尔扩域，并且 $k(\lambda)$ 具有分圆数域 $\boldsymbol{Q}(\zeta_n)$许多相似的数论性质。简言之，Hilbert 古典分圆数域的许多结果在$k(\lambda)$中都有相应的类比（见本书第 1 章）。综合上述，我们有理由把 $k(\lambda)$ 称作分圆函数域. 根据 Hayes 的结果，除了平凡的常数域扩张 $k\boldsymbol{F}_{q^n}(n\geqslant 1)$之外，分圆函数域 $k(\lambda)$（λ 为 Carlitz 模 k^{ac} 的 torsion 元素）是构作 k 的最大阿贝尔扩域的基石。因此，从80年代以来，对于分圆函数域的研究引起了数论界的关注。人们最关心的课题是：近代分圆数域理论中的丰富且深刻的结果在分圆函数域中会是怎样的情况？近20年来的研究表明，对于数域的不少结果可以给出移植到函数域上的各种尝试，例如：

建立了分圆函数域的类数解析公式（见文献[35]及本书第1章，这类似于 Kummer 和 Hasse 的类数公式）；

引人分圆单位的概念，并计算各种分圆单位群在整个单位群中的指数（见文献[7]、[16]、[36]及本书第2章，这相当于 Sinnott[51]等人的结果）；

Bernoulli 数在 $k=\boldsymbol{F}_q(T)$中的两种模拟并用来研究分圆函数域类数整除性（见文献[4]、[10]、[14]、[21]、[24]、[26]、[19]、[20]、[48]及本书第4章，相当于 Kummer 结果两种不同的移植方式）；

分圆函数域上的欧拉系并用于研究类群和分圆单位的关系

(见文献[15]及本书第3章,是 Rubin[50]的模拟);

zeta 函数一些特殊值的超越理论(于靖得出了比数域情形较圆满的完整结果). 等等.

另一方面,还有大量问题在分圆函数域中没有解决,其原因往往是由于 k 和 Q 有不同的特征,而特征为素数的域 k 比特征为零的情形会带来很大困难,所以需要有新的思想。例如说,Goss[22,27]构作了与 Hasse-Weil zeta 函数完全不同的新型 zeta 函数,Goss 和 Thakur[28],[54]继 Carlitz 之后继续深入系统地研究了函数域上各种类型的 Γ-函数,Thakur[55]用 Carlitz 模的方式给出函数域上的一种高斯和,它们在不同程度上起着古典 zeta 函数,Γ-函数以及高斯和在分圆数域研究中的作用。最近,人们也正在探索函数域上新的分析学工具(见文献[29]~[31]),期望新的工具对函数域的研究起着更大的作用。

分圆数域的近代理论(特别是 IwasawaZ_p 扩张理论和 Iwasawa 主猜想)已经成为高维几何对象算术性质的重要研究课题。类似地,分圆函数域的研究目前也已扩展到更一般情形(秩≥2的情形),这应当首先归功于 Drinfeld[9],他在70年代中期建立了函数域上的椭圆模结构(现已被称为 Drinfeld 模),并用这种方法证明了函数域上局部 Langlands 猜想的二维情形。秩为1的 Drinfeld 模就是 Carlitz 模,所以 Drinfeld 模理论是分圆函数域理论高秩的推广。我们知道,C 中的 Z-格只有秩为1和秩为2的情形,所以目前只对有理数域 Q 和虚二次域可以完全明显地构作出最大阿贝尔扩域。但是对于任意的函数域 K($k=F_q(T)$的任意有限扩域)和它的整元环 O_k,K^∞ 中可以有许多种任意秩的 O_k-格. 因此,Drinfeld 模理论比数域情形要丰富得多。这也是目前人们致力于研究 Drinfeld 模的一个原因。

本书向大家介绍分圆函数域理论,即 $F_q(T)$上秩为1的 Drinfeld 模(即 Carlitz 模)的基本数论结果,目的是总结近20年来散见于文献中的研究成果(包括作者和其他中国学者的工作). 熟悉近代分圆数域理论(例如读过 Washington[57]和 Lang[45]的书)的读

者，可以体会到分圆函数域理论和数域情形的异同，从而可以启发出来分圆函数域的许多研究课题。进而，本书也可作为进一步了解任意函数域上任意秩的 Drinfeld 模的入门书(关于一般 Drinfeld 模理论可参见文献[8]、[9]、[17]、[40]和[41]).

本书第1章介绍分圆函数域最基本的知识(相当于 Hilbert 对分圆数域的工作)；第2章讲述分圆单位，这是 Galovich、Rosen、冯克勤、程露、印林生等人工作的总结(数域情形可见文献[45]和[57])；第3章讲述分圆函数域的欧拉系(Euler System)，这是冯克勤和徐飞将 Kolyvagin 和 Rubin 的工作向函数域的移植，用来研究类群和分圆单位的联系；第4章为类数整除性，总结了 Goss、Gekeler、冯克勤、高文云等人的工作，是模拟 Kummer 理论的各种尝试，并探讨函数域情形出现的新现象；第5章在函数域上发展分析学的工具，包括 Mahler 定理的模拟、Γ-函数、高斯和、积分理论(分布与测度)，是 Goss、Thakur 等人工作的总结。这些理论目前仍处在发展阶段。最后是两个附录(高次互反律的"分圆"证明和分圆函数域的正规整基)，它们在内容上不能归于前五章中，而有自身的意义。

作者从1985年起为研究生举办过多次关于分圆函数域和 Drinfeld 模的讨论班，并且与他们一起从事这方面的研究工作。本书就是这些讨论班中的材料以及研究工作中的一部分材料的总结。作者感谢参加讨论班的中国科技大学历届研究生，他们和我曾进行过许多有益的讨论和共同从事研究工作。其中特别要感谢徐飞博士，他为本书写了第3章的初稿。我希望这本书能促使更多的同行对于分圆函数域以及一般的 Drinfeld 模理论产生兴趣，并且去试图研究其中一些重要的课题。

最后，作者感谢数学天元基金提供的资助。

冯克勤
1995年7月于中国科学技术大学

常用符号

$\boldsymbol{F}_q$	q 元有限域
p	q 的素因子
$k=\boldsymbol{F}_q(T)$	常数域为 $\boldsymbol{F}_q$ 的有理函数域
$R=\boldsymbol{F}_q[T]$	$\boldsymbol{F}_q$ 上多项式环
R_1	R 中首1多项式全体
k^{ac}	k 的代数闭包
Λ_M	Carlitz R-模 k^{ac} 中的 M-torsion 子模
$K=k(\Lambda_M)$	分圆函数域
$K^+=k(\Lambda_M)^+$	K 的最大"实"子域
O_K,O_K^+	K 和 K^+ 的整元环
U_K,U_K^+	环 O_K 和 O_K^+ 的单位群
$C(K),C^0(K),C(O_K)$	函数域 K 的除子类群，零次除子类群和理想类群
$h(K),h(O_K)$	K 的(零次)除子类数和理想类数
$R(O_K)$	K 的 regulator
χ	R 上的 Dirichlet 特征
χ^*	与 χ 相结合的本原特征
F_χ	χ 的导子(conductor)
$Z_K(U)$	函数域 K 的(Hasse-Weil)zeta 函数
$g(K)$	函数域 K 的亏格

$C_y(K^+)$	Kummer-Hilbert 分圆单位系
$C_y(\mathscr{D},K^+)$	Levesque 分圆单位系
C	Sinnott 分圆单位群
S^-	Stickelberger 理想
$\zeta_A(s)$	Goss zeta 函数
$\beta_i(T)$	Bernoulli-Goss 多项式
$e(z)$	指数函数
B_m	Bernoulli-Carlitz“数”
$[i]=T^{q^i}-T$	
$D_i=[i][i-1]^q\cdots[1]^{q^{i-1}}$	
$L_i=[i][i-1]\cdots[1]$	
$\begin{bmatrix} i \\ k \end{bmatrix}=\dfrac{D_i}{D_k L_{i-k}^{q^k}}$	
Γ_j	Gamma 函数
$\Gamma_p(z)$	P-adic Gamma 函数
g_j	高斯和
$s_i(k)=\sum\limits_{\substack{A\in R_1 \\ \deg A=i}} A^k$	幂和

目　录

CONTENTS

第 1 章

分圆函数域

§1.1 Carlitz 模和分圆函数域

设 $k=\boldsymbol{F}_q(T)$是有限域 $\boldsymbol{F}_q$ 上关于未定元 T 的有理函数域，其中 $q=p^\lambda$，p 为素数，λ 为正整数. k^{ac} 为 k 的一个固定的代数闭包，$R=\boldsymbol{F}_q[T]$是多项式环. 为了构作 k 上非平凡的阿贝尔扩张，本世纪30年代 Carlitz[1]在 k^{ac} 上引入一种 R-模结构. 我们用 End(k^{ac})表示 k^{ac}的 $\boldsymbol{F}_q$-自同态环，则有 Frobenius 自同构 F，其中

$$F(\alpha)=\alpha^q \quad (\alpha\in k^{ac}).$$

现在对 $a\in \boldsymbol{F}_q$ 定义 $\rho_a,\rho_T\in\mathrm{End}(k^{ac})$，其中

$$\rho_a(\alpha)=a\alpha,\rho_T(\alpha)=(T+F)(\alpha)=T\alpha+\alpha^q \quad (\alpha\in k^{ac}).$$

一般地，对 R 中每个多项式

$$M(T)=a_dT^d+a_{d-1}T^{d-1}+\cdots+a_0 \quad (a_i\in \boldsymbol{F}_q)$$

和 $\alpha\in k^{ac}$，则有 $\rho_M\in\mathrm{End}(k^{ac})$，其中

$$\begin{aligned}\rho_M(\alpha)&=M(T+F)(\alpha)\\&=a_d\rho_{T^d}(\alpha)+a_{d-1}\rho_{T^{d-1}}(\alpha)+\cdots+a_0\alpha,\end{aligned}$$

而

$$\begin{aligned}\rho_{T^2}(\alpha)&=\rho_T(\rho_T(\alpha))=\rho_T(T\alpha+\alpha^q)\\&=T(T\alpha+\alpha^q)+(T\alpha+\alpha^q)^q\\&=T^2\alpha+(T+T^q)\alpha^q+\alpha^{q^2},\end{aligned}$$

$$\rho_{T^n}=\rho_{T^{n-1}}(\rho_T(\alpha)).$$

这就给出了 k^{ac} 的一个 R-模结构：

$$\rho: R \to \mathrm{End}(k^{ac}), M \mapsto \rho_M,$$

称作 Carlitz 模. 传统上常把 $\rho_M(\alpha)$ 记成 α^M（当 $M=a\in \mathbf{F}_q$ 时，这个记号 $\alpha^a=\rho_a(\alpha)=a\alpha$，并不是 a 个 α 相乘，但是这种混淆今后容易区别开来）.

由定义不难看出，α^M 是关于 α 的 q-多项式，即

$$\alpha^M = \sum_{i=0}^{d} \begin{bmatrix} M \\ i \end{bmatrix} \alpha^{q^i},$$

其中 $d=\deg M$，$\begin{bmatrix} M \\ i \end{bmatrix} \in R$.

引理 1.1.1　(1) $\begin{bmatrix} M \\ 0 \end{bmatrix}=M$，$\begin{bmatrix} M \\ i \end{bmatrix}=0$（当 $i>d$ 或 $i<0$ 时），

$$\begin{bmatrix} T^{n+1} \\ i \end{bmatrix}=T\begin{bmatrix} T^n \\ i \end{bmatrix}+\begin{bmatrix} T^n \\ i-1 \end{bmatrix}^q.$$

(2) M、$N\in R$，a、$b\in \mathbf{F}_q$，则 $\begin{bmatrix} aM+bN \\ i \end{bmatrix}=a\begin{bmatrix} M \\ i \end{bmatrix}+b\begin{bmatrix} N \\ i \end{bmatrix}$.

(3) $\deg\begin{bmatrix} M \\ i \end{bmatrix}=(d-i)q^i$　$(0\leqslant i\leqslant d)$.

证明　由 Carlitz 模的定义和数学归纳法即可知.　∎

对每个 $0\neq M\in R$，$d=\deg M$，我们记

$$|M| = q^d = \#(R/(M)).$$

考虑 k^{ac} 的 M-torsion 子模

$$\Lambda_M = \{\alpha \in k^{ac}: \alpha^M = 0\},$$

由于 $u^M=\sum_{i=0}^{d}\begin{bmatrix} M \\ i \end{bmatrix}u^{q^i}$ 是关于 u 的 q^d 次多项式，它的微商为

$$(u^M)' = \left(\begin{bmatrix} M \\ 0 \end{bmatrix}u\right)' = \begin{bmatrix} M \\ 0 \end{bmatrix} = M \neq 0,$$

所以 u^M 是关于 u 的可分多项式，而 Λ_M 是此多项式的 q^d 个不同的根构成的，于是 $\#(\Lambda_M)=|M|$，即 Λ_M 是有限 R-模.

引理 1.1.2　对于 $0\neq M\in R$，有 R-模同构 $\Lambda_M\cong R/(M)$（这里 $R/(M)$ 赋以通常的 R-模结构），于是 Λ_M 是循环 R-模.

证明 对每个 $a\in \boldsymbol{F}_q^*$，易知 $\Lambda_M=\Lambda_{aM}$，$R/(M)=R/(aM)$，所以不妨设 M 是首 1 多项式. 先设 $M=P^e$，其中 $P=P(T)$ 是 R 中首 1 不可约多项式，$n=\deg P\geqslant 1$. 当 $e=1$ 时，Λ_P 是域 $M/(P)$ 上的模. 由 $\#(M/(P))=|P|=\#(\Lambda_P)$，可知 $\Lambda_P\cong M/(P)$. 现在设 $\Lambda_{P^m}\cong R/(P^m)$ $(m\geqslant 1)$，则有 R-模同态：

$$h:\Lambda_{P^{m+1}}\to \Lambda_{P^m},\quad h(\alpha)=\alpha^P.$$

由于 $\ker h=\Lambda_P$，$\#(\Lambda_{P^{m+1}})=|P^{m+1}|=\#(\Lambda_{P^m})\#(\Lambda_P)$，可知 h 是满同态. 于是有 $\lambda\in\Lambda_{P^{m+1}}$，使得 λ^P 是 R-模 Λ_{P^m} 的生成元. 对每个 $\mu\in \Lambda_{P^{m+1}}-\{0\}$，则存在 $A\in R$，使得 $\mu^P=(\lambda^P)^A=\lambda^{PA}$，于是 $\mu-\lambda^A\in \mathrm{her}h=\Lambda_P$. 另一方面，由于 λ^P 是 Λ_{P^m} 的生成元，从而 $\lambda^{P^m}\in\Lambda_P-\{0\}$，即 λ^{P^m} 是 Λ_P 的生成元，于是有 $B\in R$，使得 $\mu-\lambda^A=\lambda^{P^mB}$，即 $\mu=\lambda^{A+P^mB}$. 这就证明了 λ 生成模 $\Lambda_{P^{m+1}}$，即 $\Lambda_{P^{m+1}}$ 是循环 R-模. 考虑 R-模单同态 $R/(P^{m+1})\to\Lambda_{P^{m+1}}$，$A\mapsto\lambda^A$. 由 $\#(\Lambda_{P^{m+1}})=|P^{m+1}|=\#(R/(P^{m+1}))$，即知 $\Lambda_{P^{m+1}}\cong R/(P^{m+1})$. 这就对 $M=P^e$ 的情形证明了引理.

对于一般情形，设 $M=\prod\limits_{i=1}^{g}P_i^{e_i}$，其中 $P_1,\cdots,P_g$ 是 R 中不同的首 1 不可约多项式. 则 $\sum\limits_{i=1}^{g}\Lambda_{P_i^{e_i}}$ 是 Λ_M 的 R-子模，由中国剩余定理可知 $\sum\limits_{i=1}^{g}\Lambda_{P_i^{e_i}}$ 是直和. 于是

$$\#\Big(\sum_i\Lambda_{P_i^{e_i}}\Big)=\prod_{i=1}^{g}|P_i|^{e_i}=|M|=\#(\Lambda_M).$$

这就表明

$$\Lambda_M\cong\sum_{i=1}^{g}\Lambda_{P_i^{e_i}}\ (\text{直和})\cong\sum_{i=1}^{g}R/(P_i^{e_i})\ (\text{直和})\cong R/(M).$$

从而证明了引理 1.1.2. ▌

Λ_M 中元素称作 *M-torsion 元素*，循环 R-模 Λ_M 的每个生成元都称作*本原 M-torsion 元素*. 由引理 1.1.2 可知道，对每个本原 M-torsion 元素 λ，有

$$\Lambda_M = \{\lambda^A; A \in R/(M)\},$$

并且 λ^A 是本原 M-torsion 元素当且仅当 $(A,M)=1$ （即 $A\in(R/(M))^*$），其中 $(R/(M))^*$ 表示有限环 $R/(M)$ 中乘法可逆元素构成的单位群. 记 $\Phi(M)=\#((R/(M)^*)$，则 $\Phi(M)$ 是通常欧拉函数 $\varphi(m)$ （它表示 $1,2,\cdots,m$ 之间与 m 互素的正整数个数）的模拟. 由中国剩余定理可知

$$\Phi(M) = |M| \cdot \prod_{P|M}\left(1 - \frac{1}{|P|}\right),$$

其中 P 过 M 的全体首 1 不可约因子. 此式是公式

$$\varphi(m) = m\prod_{p|m}\left(1 - \frac{1}{p}\right)$$

的模拟.

定义 1.1.3 设 M 是 $R=\boldsymbol{F}_q[T]$中首 1 多项式，将 Λ_M 中所有元素添加到域 $k=\boldsymbol{F}_q(T)$上而得到的扩域 $k(\Lambda_M)$称作分圆函数域，M 称作此域的导子(conductor).

令 λ 是一个本原 M-torsion 元素，则

$$u^M = \prod_{\alpha\in \Lambda_M}(u - \alpha) = \prod_{A\in (R/(M))}(u - \lambda^A).$$

由于 u^M 是可分多项式，所以 $k(\Lambda_M)/k$ 是有限伽罗华扩张. 由于每个根 λ^A 都是 λ 的多项式(系数属于 R)，所以 $k(\Lambda_M)=k(\lambda)$. 记

$$G = G_M = \mathrm{Gal}(k(\Lambda_M)/k)$$

为扩张 $k(\Lambda_M)/k$ 的伽罗华群，则每个自同构 $\sigma\in G$ 由它在 λ 上的作用所完全决定. 易知 $\sigma(\lambda)$仍是本原 M-torsion 元素(因为 $\sigma(\lambda^T)=\sigma(T\lambda-\lambda^q)=T(\sigma(\lambda))-(\sigma(\lambda))^q=\sigma(\lambda)^T$，从而对每个 $A\in R$，$\sigma(\lambda^A)=\sigma(\lambda)^A$)，于是

$$\sigma(\lambda) = \lambda^A,\ A \in (R/(M))^*.$$

我们把这个自同构记成 σ_A，则

$$\sigma_A\sigma_B(\lambda) = \sigma_A(\lambda^B) = \lambda^{AB} = \sigma_{AB}(\lambda).$$

这就表明有群的单同态

$$G \to (R/(M))^*,\ \sigma_A \mapsto A.$$

特别地，G 同构于 $(R/(M))^*$ 的一个子群，所以 $k(\Lambda_M)/k$ 是阿贝尔扩张，并且 $[k(\Lambda_M):k]=|G|\leqslant\Phi(M)$。我们的下一个目标是证明

$$G\cong(R/(M))^*,$$

即对每个 $A\in(R/(M))^*$，$\lambda\mapsto\lambda^A$ 均是 $k(\Lambda_M)$ 的 k-自同构，这也等价于 $[k(\Lambda_M):k]=\Phi(M)$，或者等价于 u^M 是 k 上的不可约多项式。为证此论断，我们需要研究 R 中每个首 1 不可约多项式 P（即 k 的有限素除子）在分圆函数域 $k(\Lambda_M)$ 中的分解情况。

引理 1.1.4　设 $M=P^n$，其中 P 是 R 中首 1 不可约多项式，$n\geqslant1$。则 P 在 $K=k(\Lambda_M)$ 中完全分歧，并且 R 中其他的首 1 不可约多项式在 $k(\Lambda_M)$ 中不分歧。

证明　令 λ 是本原 M-torsion 元素，则 $k(\Lambda_M)=k(\lambda)$，而 λ 是关于 u 的多项式 $f(u)=u^{P^n}/u^{P^{n-1}}$ 的根。由引理 1.1.1 知道

$$P=\begin{bmatrix}P^n\\0\end{bmatrix}\Big/\begin{bmatrix}P^{n-1}\\0\end{bmatrix}=f(0)=\prod_{A\in(R/(M))^*}(-\lambda^A).\quad(1.1.1)$$

以 O_K 表示 R 在 K 中的整闭包，则 $\lambda^A\in O_K$。由于 λ^A 是 λ 的 q-多项式（系数属于 R），因此 $\lambda^A/\lambda\in R[\lambda]\subseteq O_K$。如果 $A\in(R/(M))^*$，即 $(A,M)=1$ 时，有 $B\in R$ 使得 $AB\equiv1\pmod M$。因此 $\lambda/\lambda^A=(\lambda^A)^B/\lambda^A\in R[\lambda^A]\subseteq O_K$。这就表明 λ^A/λ 为 O_K 中的单位，于是 O_K 中理想 (λ^A) 和 (λ) 相同。由(1.1.1)式可知

$$P=\mathscr{P}^{\Phi(M)},$$

其中 $\mathscr{P}=(\lambda)$。以 e 表示 P 在 $K=k(\Lambda_M)$ 中的分歧指数，则

$$e\leqslant[K:k]\leqslant\Phi(M)\leqslant e.$$

于是 $[K:k]=\Phi(M)=e$，即 P 在 K 中完全分歧，并且 $\mathscr{P}=(\lambda)$ 是 O_K 的素理想。由于 $\deg f(u)=|P^n|-|P^{n-1}|=\Phi(P^n)=[K:k]$，可知 $f(u)$ 是 λ 在 k 上的极小多项式。将等式 $f(u)u^{P^{n-1}}=u^{P^n}$ 两端对 u 微商，得到

$$f'(u)u^{P^{n-1}}+f(u)P^{n-1}=P^n.$$

代入 $u=\lambda$，可知 $f'(\lambda)\lambda^{P^{n-1}}=P^n$。由 $[K:k]=\Phi(M)$ 可知，对 $M=P^n$ 的情形 $G_M=\{\sigma_A:A\in(R/(M))^*\}$，以 $N=N_K/k$ 表示关于扩张

K/k的范映射,即对于$\alpha\in K$,有

$$N(\alpha)=\prod_{\sigma\in G}\sigma(\alpha)=\prod_{A\in(R/(M))^*}\sigma_A(\alpha)\in k.$$

由(1.1.1)式可知$N(\lambda)=P$. 由于$\lambda^{P^{n-1}}$是本原P-torsion 元素,所以

$$\begin{aligned}N(\lambda^{P^{n-1}})&=N_{k(\Lambda_P)/k}(N_{K/k(\Lambda_P)}(\lambda^{P^{n-1}}))\\&=N_{k(\Lambda_P)/k}(\lambda^{P^{n-1}})^{[K:k(\Lambda_P)]}\\&=N_{k(\Lambda_P)/k}(\lambda^{P^{n-1}})^{|P|^{n-1}}=P^{|P|^{n-1}}.\end{aligned}$$

对$f'(\lambda)\lambda^{P^{n-1}}=P^n$两端取范数$N$,得到

$$N(f'(\lambda))N(\lambda^{P^{n-1}})=N(P^n)=P^{n\Phi(P^n)}.$$

因此$N(f'(\lambda))=P^m$,其中$m=n\Phi(P^n)-|P|^{n-1}$. 熟知O_K的判别式$D(K)$是$N(f'(\lambda))$的因子,并且根据 Dedekind 的判别式定理:R中首1不可约多项式Q在K中分歧,当且仅当$Q|D(K)$. 这就表明当$Q\neq P$时,Q在K中不分歧. ▌

定理 1.1.5　设M是R中首1多项式,则$k(\Lambda_M)/k$是$\Phi(M)$次阿贝尔扩张,并且其伽罗华群同构于$(R/(M))^*$.

证明　我们只需证明

$$[k(\Lambda_M):k]=\Phi(M).$$

设$M=\prod_{i=1}^{g}P_i^{e_i}$,其中$P_1,\cdots,P_g$为$R$中不同的首1不可约多项式,$e_i\geqslant1$. 记$K_i=k(\Lambda_{P_i^{e_i}})(1\leqslant i\leqslant g)$,根据引理1.1.4,$P_1$在$K_1$中完全分歧而在$K_2$中不分歧,于是$K_1\cap K_2=k$,从而$[K_1K_2:k]=[K_1:k][K_2:k]$. 类似地,$P_3$在$K_1K_2$中不分歧而在$K_3$中完全分歧,于是$[K_1K_2K_3:k]=[K_1K_2:k][K_3:k]$. 依此类推,可知

$$[K_1K_2\cdots K_g:k]=\prod_{i=1}^{g}[K_i:k]=\prod_{i=1}^{g}\Phi(P_i^{e_i})=\Phi(M).$$

进而由$\Lambda_{P_i^{e_i}}\subseteq\Lambda_M$,可知$K_1K_2\cdots K_g\subseteq k(\Lambda_M)$. 于是

$$\Phi(M)\geqslant[k(\Lambda_M):k]\geqslant[K_1K_2\cdots K_g:k]=\Phi(M).$$

这就表明$[k(\Lambda_M):k]=\Phi(M)$(并且$k(\Lambda_M)=K_1K_2\cdots K_g$). ▌

注记 将有理函数域$k=F_q(T)$和多项式环$R=F_q[T]$分别看成是有理数域Q和整数环Z的模拟,则M-torsion子模Λ_M可看成是复m次单位根群$\mu_m=\{e^{\frac{2\pi i}{m}s}\mid 0\leqslant s\leqslant m-1\}$的模拟.我们知道,分圆数域$Q(\mu_m)$是$Q$的$\varphi(m)$次阿贝尔扩张,并且它的伽罗华群$G$自然同构于$(Z/mZ)^*$,其中每个$a\in(Z/mZ)^*$对应于自同构$\sigma_a$,$\sigma_a$把每个$m$次本原单位根$\zeta$映成$\zeta^a$.而定理1.1.5就是这个结果在分圆函数域的模拟.往后我们还会看到,分圆函数域的许多结果与分圆数域是类似的.

以O_K表示R在$K=k(\Lambda_M)$中的整闭包,称作K的*整元环*.这是主理想整环R上的自由模,秩为$[K:k]=\Phi(M)$.O_K的每个元素称作K中的*整元素*,O_K的每组R-基称作K的*整基*.对于分圆数域$Q(\zeta_m)$ $\left(\zeta_m=e^{\frac{2\pi i}{m}}\right)$,熟知其整数环为$Z[\zeta_m]$,类似地,有如下定理:

定理1.1.6 设M为R中首1多项式,$K=k(\Lambda_M)$,$s=\Phi(M)=[K:k]$,则$O_K=R[\lambda]$,其中λ是一个本原M-torsion元素.换句话说,$1,\lambda,\lambda^2,\cdots,\lambda^{s-1}$是$O_K$的一组整基.

证明 先设$M=P^e$.由于$K=k(\lambda)$,可知$1,\lambda,\lambda^2,\cdots,\lambda^{s-1}$是向量空间$K$的一组$k$-基.所以每个整元素$\alpha\in O_K$均可唯一地表示成

$$\alpha=t_0+t_1\lambda+\cdots+t_{s-1}\lambda^{s-1}\quad(t_i\in k).$$

我们的目的是证明$t_i\in R(0\leqslant i\leqslant s-1)$.将$K/k$的自同构$\sigma_A$作用于上式两端,得到

$$\sigma_A(\alpha)=t_0+t_1\lambda^A+\cdots+t_{s-1}(\lambda^A)^{s-1}\quad(A\in(R/(M))^*).$$

这$s=\Phi(M)$个方程看成关于$t_i(0\leqslant i\leqslant s-1)$的线性方程组,解出(由Cramer法则)

$$t_i=\gamma_i/\delta\quad(0\leqslant i\leqslant s-1),$$

其中

$$\delta=\det(C_{A,k}),C_{A,k}=(\lambda^A)^k\quad(0\leqslant k\leqslant s-1,A\in(R/(M))^*),$$

而γ_i是整元素方阵的行列式,所以$\gamma_i\in O_K$ $(0\leqslant i\leqslant s-1)$.由于$(C_{A,k})$是Vandermonde方阵,可知

$$\delta^2=\pm\prod_{\substack{A,B\in(R/(M))^*\\A\neq B}}(\lambda^A-\lambda^B).$$

另一方面,当 $M=P^r$ 时,引理 1.1.4 证明了

$$f(u)=u^{P^r}/u^{P^{r-1}}=\prod_{B\in(R/(M))^*}(u-\lambda^B)$$

是 λ 的极小多项式,于是

$$f'(\lambda^A)=\prod_{\substack{B\in(R/(M))^*\\B\neq A}}(\lambda^A-\lambda^B),$$

$$N_{K/k}(f'(\lambda))=\prod_{A\in(R/(M))^*}f'(\lambda^A)=\pm\delta^2.$$

引理 1.1.4 证明了 $N_{K/k}(f'(\lambda))=P^r$(对某个 $r\geqslant1$). 于是

$$t_i=\pm\gamma_i\delta/\delta^2=\pm\gamma_i\delta/P^r,$$

其中 $\gamma_i\delta\in O_K$. 但是 $\gamma_i\delta=t_iP^r\in k$,因此 $\gamma_i\delta\in O_K\cap k=R$. 这就表明 k 中元素 $t_i(0\leqslant i\leqslant s-1)$的分母多项式最多是 P^r. 于是 α 可以写成

$$\alpha=P^{-r}(A_0+A_1\lambda+\cdots+A_{s-1}\lambda^{s-1})\quad(A_i\in R).\tag{1.1.2}$$

引理 1.1.4 还证明了 $\mathscr{P}=(\lambda)$是 O_K 的素理想,并且 $P=\mathscr{P}^s$. 我们以 v_p 表示 K 中的标准 $\mathscr{P}$-adic 指数赋值,$v_p(\lambda)=1$. 由 $P=\mathscr{P}^s$ 可知 $v_p(P)=s$. 于是 $v_p(A_i)\equiv0 \pmod s$ $(0\leqslant i\leqslant s-1)$. 所以

$$v_p(A_i\lambda^i)\equiv v_p(\lambda^i)\equiv i\pmod s\quad(0\leqslant i\leqslant s-1).$$

这就表明公式(1.1.2)中右端诸项有不同的 $\mathscr{P}$-adic 指数赋值. 所以

$$v_p(\alpha)=\min_{0\leqslant i\leqslant s-1}\{v_p(P^{-r}A_i\lambda^i)\}.$$

但是 $\alpha\in O_K$,于是

$$0\leqslant v_p(\alpha)\leqslant v_p(P^{-r}A_i\lambda^i)=v_p(A_i)+i-rs(0\leqslant i\leqslant s-1).$$

这就表明 $v_p(A_i)\geqslant rs$,即 $P^r|A_i$ $(0\leqslant i\leqslant s-1)$,于是 $t_i=P^{-r}A_i\in R$ $(0\leqslant i\leqslant s-1)$. 从而对于 $M=P^r$ 的情形证明了定理.

对于一般情形,$M=\prod_{i=1}^{g}P_i^{r_i}$,其中 $P_i(1\leqslant i\leqslant g)$是 R 中不同的首1不可约多项式. 令 $K_i=k(\Lambda_{P_i^{r_i}})$ $(1\leqslant i\leqslant g)$,引理1.1.4中证明

了域 K_i 的判别式 $D(K_i)$ 为 P_i 的方幂. 所以 $D(K_i)(1\leqslant i\leqslant g)$ 是两两互素的. 熟知在这种情形下, 必然 $O_{K_iK_j}=O_{K_i}O_{K_j}$. 于是 $O_K=O_{K_1}O_{K_2}\cdots O_{K_g}$. 记 λ_i 为本原 $P_i^{e_i}$-torsion 元素, 则前面已证明了 $O_{K_i}=R[\lambda_i]$ $(1\leqslant i\leqslant g)$. 于是 $O_K=R[\lambda_1,\lambda_2,\cdots,\lambda_g]=R[\lambda]$. 这就证明了定理 1.1.6. ▌

注记 让我们回忆一下判别式的定义. 记 K/k 是有限伽罗华扩张, $s=[K:k]$, $G=\{\sigma_1,\cdots,\sigma_s\}$ 是 K/k 的伽罗华群. 对于 O_K 的一组整基 $w_1,w_2,\cdots,w_s$, 则

$$D=\det(\sigma_i(w_j))^2_{1\leqslant i,j\leqslant s}$$

是 $R=F_q(T)$ 中元素, 并且作为环 R 中理想 $(D)=DR$ 是域 K 的特性, 而与整基 $w_1,\cdots,w_s$ 的选取方式无关. 理想 (D) (或者 D) 称为域 K 的判别式, 表示成 $D(K)$. 对于分圆函数域 $K=k(\Lambda_M)$, 当 $M=P^n$ 时, 由定理1.1.6和引理1.1.4的证明可知

$$\begin{aligned}D(K)&=\det((\lambda^A)^k)^2\quad (A\in(R/(M))^*,0\leqslant k\leqslant\Phi(M)-1)\\&=P^r,\end{aligned}$$

其中 $r=n\Phi(P^n)-\Phi(P^n)/\Phi(P)$.

一般地, 若 K_1 和 K_2 均是 k 的有限伽罗华扩张, $K=K_1K_2$, $m=[K_1:k]$, $n=[K_2:k]$, 而 $\{\omega_1,\cdots,\omega_m\}$ 和 $\{\lambda_1,\cdots,\lambda_n\}$ 分别是 K_1 和 K_2 的一组整基. 如果 $(D(K_1),D(K_2))=1$, 则

$$\begin{aligned}O_K=O_{K_1}O_{K_2}&=\Big(\sum_{i=1}^m R\omega_i\Big)\Big(\sum_{j=1}^n R\lambda_j\Big)\\&=\sum_{i=1}^m\sum_{j=1}^n R\omega_i\lambda_j\ (\text{直和}).\end{aligned}$$

这表明 $\{\omega_i\lambda_j\mid 1\leqslant i\leqslant m,1\leqslant j\leqslant n\}$ 是 K 的一组整基. 由此可得出 $D(K)=D(K_1)^nD(K_2)^m$. 利用这个结果和上面计算出的关于 $k(\Lambda_{P^n})$ 的判别式, 可得到对一般的 M, $K=k(\Lambda_M)$ 的判别式为

$$D(K)=M^{\Phi(M)}\Big/\prod_{P\mid M}P^{\Phi(M)/\Phi(P)}.$$

这个公式与分圆数域的情形是类似的.

§1.2 素除子

有理函数域 $k=\mathbf{F}_q(T)$ 的素除子分为有限素除子(即 $R=\mathbf{F}_q[T]$ 中所有首1不可约多项式)和无限素除子 $\infty=\left(\frac{1}{T}\right)$. 本节要考查这些素除子在分圆函数域中是如何分解的. 先考查有限素除子 P 的情形.

定理1.2.1 设 $M=P^nN$, $(P,N)=1$, $n\geqslant 0$, 则 P 在分圆函数域 $K=k(\Lambda_M)$ 中的分解式为

$$P=(\mathscr{P}_1\mathscr{P}_2\cdots\mathscr{P}_g)^e,$$

其中 $e=\Phi(P^n)$, $g=\dfrac{\Phi(N)}{f}$, 而 f 是 P 在群 $(R/(N))^*$ 中的阶(即 f 是满足 $P^r\equiv 1\pmod{N}$ 的最小正整数 r), e,f,g 分别是 P 在 K 中的分歧指数、剩余类域次数和分解次数.

证明 以 K' 表示 P 在 K 中的惰性域(即 P 在 K 中的最大不分歧子域), 则 $[K:K']=e$, $[K':k]=fg$. 根据引理1.1.4, P 在 K 的子域 $k(\Lambda_{P^n})$ 中完全分歧, 于是 $e\geqslant[k(\Lambda_{P^n}):k]=\Phi(P^n)$. 另一方面, P 在 $k(\Lambda_N)$ 中不分歧, 所以

$$\begin{aligned}e\leqslant[K:k(\Lambda_N)]&=[K:k]/[k(\Lambda_N):k]\\&=\Phi(M)/\Phi(N)=\Phi(P^n).\end{aligned}$$

于是 $e=\Phi(P^n)$, 并且 $K'=k(\Lambda_N)$.

P 在 K' 中的剩余类域的次数和分解次数就是 f 和 g, 于是 $fg=\Phi(N)$. 我们只需决定 f. 设 λ 是一个本原 N-torsion 元素, 则 K'/k 的伽罗华群为

$$G=\{\sigma_A:A\in(R/(N))^*\}\cong(R/(N))^*,$$

其中 $\sigma_A(\lambda)=\lambda^A$. 我们知道, f 即是 G 中元素 $\sigma=\left(\dfrac{K'/k}{P}\right)$ (关于 P 的 Frobenius 自同构)的阶. 熟知 σ 可由下面的同余式所刻划:

$$\sigma(a)\equiv a^{|P|}\pmod{\mathscr{P}}\quad(\text{对每个 } a\in O_{K'}),\qquad(1.2.1)$$

这里 $\mathscr{P}$ 是 P 在 K' 中一个固定的扩充素除子. 记 $\sigma=\sigma_A$, 我们来决

定$(R/(N))^*$中元素 A. 在(1.2.1)中取 $u=\lambda$,便得到

$$\lambda^A \equiv \lambda^{|P|} \pmod{\mathscr{P}}. \tag{1.2.2}$$

现在设 μ 是一个本原 P-torsion 元素,则

$$u^P = u \prod_{B\in(R/(P))^*} (u-\mu^B).$$

引理1.1.4表明,(μ^B)均是 P 在 $k(\Lambda_P)$中的唯一扩充素除子 $\mathscr{P}'$. 所以关于 u 的多项式 u^P 除了最高项 $u^{|P|}$之外,其余诸项的系数均被 $\mathscr{P}'$除尽. 但是这些系数都属于 R,所以它们均被 P 除尽. 这就表明 $u^P\equiv u^{|P|} \pmod{P}$. 再由(1.2.2)式和 $\mathscr{P}|P$,可知

$$\lambda^P\equiv \lambda^{|P|} \equiv \lambda^A \pmod{\mathscr{P}},$$

于是

$$\lambda^{A-P}= \lambda^A - \lambda^P \equiv 0 \pmod{\mathscr{P}}.$$

现在我们证明

$$A \equiv P \pmod{N}.$$

因为若不然,则有$0\neq\lambda^{A-P}\in\Lambda_N$. 于是$\lambda^{A-P}$是关于$u$的多项式 u^N/u的根. 引理1.1.1表明u^N/u的常数项为$\begin{bmatrix}N\\0\end{bmatrix}=N$,于是 $\mathscr{P}\,|\,\lambda^{A-P}\,|\,N$,从而 $P\,|\,N$,这与假设$(P,N)=1$相矛盾. 这就表明 $A\equiv P \pmod{N}$,即 $\sigma=\sigma_A=\sigma_P$. 由前述,f 是元素 σ_P 的阶,即是 P 在$(R/(N))^*$中的阶,这就完成了定理1.2.1的证明. ▌

定理1.2.1与分圆数域中素数分解规律是完全类似的. 现在我们考虑 k 中无限素除子$\infty=\left(\frac{1}{T}\right)$在分圆函数域 $K=k(\Lambda_M)$中的分解情况. 我们知道这是局部性质,即考虑 k 对于素除子∞的完备化域 $k_\infty=\boldsymbol{F}_q\left(\left(\frac{1}{T}\right)\right)$,以 v_∞表示 k 和 k_∞中标准指数赋值,$v_\infty\left(\frac{1}{T}\right)=1$. 固定 v_∞到 $K=k(\Lambda_M)$中的一个扩充(仍记成 v_∞),如果本原 M-torsion 元素 λ 的极小多项式 $f(u)$在 k_∞上分解成

$$f(u) = f_1(u)f_2(u)\cdots f_g(u),$$

其中 $f_1,\cdots,f_g$ 是 $k_\infty[u]$中的首1不可约多项式,则∞在 K 中有 g 个扩充. 由于 K/k 是阿贝尔扩张,可知这 g 个扩充有同样的分歧指数 e 和剩余类域次数 f,并且 $\deg f_i(u)=ef\quad(1\leqslant i\leqslant g)$.

为了研究多项式 $f(u)$ 在局部域 k_∞ 上的分解，我们需要以下引理：

牛顿折线引理 设 F 是离散赋值域，v 是 F 中的指数赋值，

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in F[X],\ n \geqslant 1,\ a_n \neq 0.$$

以 $w_1,\cdots,w_n$ 表示 $f(X)$ 在 F 的某个代数闭包 F^{ac} 中的根，v 在 F^{ac} 中的某个扩充仍记为 v. 如果 $f(X)$ 的牛顿折线的顶点依次为

$$Q_0 = P_0,\ Q_1 = P_{r_1},\ Q_2 = P_{r_1+r_2},\ \cdots,\ Q_g = P_{r_1+r_2+\cdots+r_g}$$

$$(r_1 + r_2 + \cdots + r_g = n),$$

其中

$$P_i = (i, v(a_i)) \quad (0 \leqslant i \leqslant n),$$

（所谓 $f(X)$ 的牛顿折线是平面上这些点的一部分连成的一条凸折线，使得所有点 P_i 均在此折线的上方）. 以 l_i 表示折线中边 $\overline{Q_{i-1}Q_i}$ 的斜率，则

(1) 在 $f(X)$ 的 n 个根 $w_1,\cdots,w_n$ 当中，共有 r_1 个根 w 满足 $v(w)=l_1$，共有 r_2 个根满足 $v(w)=l_2,\cdots$，最后，共有 r_g 个根满足 $v(w)=l_g$.

(2) 以 F_v 表示赋值域 F 对于 v 的完备化，则对于每个 i $(1\leqslant i\leqslant g)$，

$$\prod_{\substack{j=1 \\ v(w_j)=l_i}}^{n} (X - w_j) \in F_v[X].$$

证明 见文献[58]. ∎

现在证明以下定理：

定理1.2.2 (1) 无限素除子 ∞ 在 $K=k(\Lambda_M)$ 中的分歧指数、剩余类域次数和分解次数分别为

$$e = q - 1, f = 1 \text{ 和 } g = \Phi(M)/(q - 1).$$

(2) 对于所有本原 M-torsion 元素 $\lambda, v_\infty(\lambda)$ 的最大值为 $\deg M - \dfrac{q}{q-1}$.

证明 先考虑 $M=P$ 的情形. 记 $d=\deg P$，对每个本原 P-torsion 元素 $\lambda, K=k(\Lambda_P)=k(\lambda)$，$\lambda$ 在 k 上的极小多项式为

$$F(u)=u^P/u=\sum_{i=0}^{d}\begin{bmatrix}P\\ i\end{bmatrix}u^{q^i-1},$$

此多项式的每一项$\begin{bmatrix}P\\ i\end{bmatrix}u^{q^i-1}$给出平面上的点：

$$P_i=\left(q^i-1,v_\infty\left(\begin{bmatrix}P\\ i\end{bmatrix}\right)\right)=\left(q^i-1,-\deg\begin{bmatrix}P\\ i\end{bmatrix}\right)$$

$$=(q^i-1,-(d-i)q^i)\quad(0\leqslant i\leqslant d),$$

而线段$\overline{P_iP_{i+1}}$的斜率为

$$l_i=\frac{-(d-i-1)q^{i+1}+(d-i)q^i}{q^{i+1}-q^i}=\frac{q}{q-1}+i-d$$

$$(0\leqslant i\leqslant d-1).$$

由于$l_0<l_1<\cdots<l_{d-1}$，可知$\overline{P_0P_1}$是牛顿折线的一条边，由上述引理便知有$q-1$个本原P-torsion元素$\lambda_1,\cdots,\lambda_{q-1}$，使得$v_\infty(\lambda_i)=-l_0=d-\frac{q}{q-1}$，并且$\prod_{i=1}^{q-1}(u-\lambda_i)\in k_\infty[u]$. 这就表明了$ef\leqslant q-1$. 另一方面，$v_\infty(\lambda_1)\mathbf{Z}=\frac{1}{q-1}\mathbf{Z}$，可知$e\geqslant q-1$. 于是$e=q-1$，$f=1$，$g=\frac{\Phi(P)}{q-1}$，这就证明了(1). 进而由上述引理知对每个本原$P$-torsion元素$\lambda$，均有$v_\infty(\lambda)=-l_i\leqslant -l_0=d-\frac{q}{q-1}$，这就证明了(2).

再考虑$M=P^n(n\geqslant 2)$的情形. 我们已经知道有本原P-torsion元素μ，使得$v_\infty(\mu)=d-\frac{q}{q-1}$. 多项式

$$G(u)=u^{P^{n-1}}-\mu=\sum_{i=0}^{d(n-1)}\begin{bmatrix}P^{n-1}\\ i\end{bmatrix}u^{q^i}-\mu\in k(\Lambda_P)[u]$$

的每个根λ都是本原P^n-torsion元素，并且$k(\Lambda_{P^n})=k(\lambda)$. $G(u)$的诸项给出平面上$d(n-1)+2$个点：

$$A_{-1}=(0,v_\infty(\mu))=\left(0,d-\frac{q}{q-1}\right),$$

$$A_i=\left(q^i,v_\infty\left(\begin{bmatrix}P^{n-1}\\ i\end{bmatrix}\right)\right)=(q^i,-((n-1)d-i)q^i)$$

$$(0 \leqslant i \leqslant d(n-1)).$$

$\overline{A_{-1}A_0}$的斜率为 $l_0=-nd+\frac{q}{q-1}$，而当 $i\geqslant 0$时，$\overline{A_iA_{i+1}}$的斜率为 $\frac{q}{q-1}+i-(n-1)d>l_0$. 从而$\overline{A_{-1}A_0}$是牛顿折线的一部分. 这表明存在本原 P^n-torsion 元素 λ，使得 $v_\infty(\lambda)=-l_0=nd-\frac{q}{q-1}=\deg P^n-\frac{q}{q-1}$，并且 $u-\lambda\in k(\Lambda_P)_{\mathscr{P}}$，其中 $\mathscr{P}$ 是 $k(\Lambda_P)$中赋值 v_∞对应的素除子. 这表明 $G(u)$在 $k(\Lambda_P)_{\mathscr{P}}$ 上完全分解成$|P^{n-1}|$个一次因子的乘积. 于是 $\mathscr{P}$ 在 $k(\Lambda_{P^n})$上的三个参数为

$$e'=1,\ f'=1,\ g'=|P^{n-1}|.$$

但是∞在 $k(\Lambda_P)$上的三个参数为

$$e''=q-1,\ f''=1,\ g''=\frac{\Phi(P)}{q-1},$$

于是∞在 $k(\Lambda_{P^n})$中的三个参数为

$$e=e'e''=q-1,\ f=f'f''=1,\ g=g'g''=\frac{\Phi(P^n)}{q-1}.$$

最后，对每个本原 P^n-torsion 元素 λ'，存在 $A\in R$，$(A,P)=1$，$\deg A<\deg P^n=dn$，使得

$$\lambda'=\lambda^A=\sum_{i=0}^{\deg A}\begin{bmatrix}A\\ i\end{bmatrix}\lambda^{q^i}.$$

由于

$$v_\infty\left(\begin{bmatrix}A\\ i\end{bmatrix}\lambda^{q^i}\right)=-(\deg A-i)q^i+q^i\left(nd-\frac{q}{q-1}\right)$$
$$=q^i\left(nd-\deg A+i-\frac{q}{q-1}\right)\quad(0\leqslant i\leqslant \deg A),$$

其中只有 $i=0$时达到最小值 $nd-\deg A-\frac{q}{q-1}$. 因此

$$v_\infty(\lambda')=v_\infty(\lambda^A)$$
$$=nd-\deg A-\frac{q}{q-1}\leqslant nd-\frac{q}{q-1}=v_\infty(\lambda).$$

这就对于 $M=P^n$ 的情形证明了定理.

最后讨论一般情形:对于 M 的不同首1不可约因子的个数 s 进行归纳. 以上证明了 $s=1$的情形. 现设 $s\geqslant 2$,并且定理对于小于 s 的情形是成立的. 记 $M=P^nN,(P,N)=1,n\geqslant 1$. 由归纳假设,$\infty$ 在 $k(\Lambda_N)$中的三个参数分别为 $e'=q-1,f'=1$和$g'=\dfrac{\Phi(N)}{q-1}$,并且存在本原 N-torsion 元素 μ,使得 $v_\infty(\mu)=\deg N-\dfrac{q}{q-1}$. 记 $\mathscr{P}$ 为 $k(\Lambda_N)$中对应于赋值∞的素除子,则多项式

$$H(u)=u^{P^n}-\mu=\sum_{i=0}^{dn}\begin{bmatrix}P^n\\ i\end{bmatrix}u^{q^i}-\mu\in k(\Lambda_N)[u]$$

的诸项给出平面上 $dn+2$个点($d=\deg P$):

$$B_{-1}=(0,v_\infty(\mu))=\left(0,\deg N-\frac{q}{q-1}\right),$$

$$B_i=(q^i,-(nd-i)q^i)\quad(0\leqslant i\leqslant nd).$$

可知 $H(u)$的牛顿折线包含线段$\overline{B_{-1}B_0}$,于是 $H(u)$有根 $\lambda\in k(\Lambda_N)_{\mathscr{P}}$,并且

$$v_\infty(\lambda)=nd+\deg N-\frac{q}{q-1}=\deg M-\frac{q}{q-1}.$$

由 $\lambda^M=\mu^N=0$可知 λ 是 M-torsion 元素. 进而对每个 $A\in R,0\leqslant\deg A<\deg M$,与上面一样,可知

$$v_\infty(\lambda^A)=\deg M-\deg A-\frac{q}{q-1}.$$

特别地,$\lambda^A\neq 0$,即 λ 是本原 M-torsion 元素. 这就表明 $\mathscr{P}$ 在 $k(\Lambda_M)$中的三个参数分别为 $e''=1,f''=1$和 $g''=\dfrac{\Phi(M)}{\Phi(N)}$. 于是$\infty$在 $k(\Lambda_M)$中的分解特性为 $e=e'e''=q-1,f=f'f''=1$和 $g=g'g''=\dfrac{\Phi(M)}{q-1}$. 并且由上述可知,对本原 M-torsion 元素 $\lambda,v_\infty(\lambda)$的最大值是 $\deg M-\dfrac{q}{q-1}$. ▌

根据定理1.2.2,k 中无限素除子$\infty=\left(\dfrac{1}{T}\right)$在 $K=k(\Lambda_M)$中分解成

$$\infty = (\mathscr{P}_1 \cdots \mathscr{P}_g)^e,$$

其中 $e=q-1, g=\frac{\Phi(M)}{q-1}$. 我们称 $\mathscr{P}_1, \cdots, \mathscr{P}_g$ 是 K 中的无限素除子，而 R 中每个有限素除子 P 在 K 中的扩充称作 K 的有限素除子. 取定 K 中一个无限素除子 $\mathscr{P}$，以 $v_{\mathscr{P}}$ 表示 K 对于 $\mathscr{P}$ 的标准指数赋值，即 $v_{\mathscr{P}}(K^*)=\mathbf{Z}$，则对于 $\alpha \in K^*$，有

$$v_{\mathscr{P}}(\alpha) = e v_{\infty}(\alpha) = (q-1) v_{\infty}(\alpha).$$

定理1.2.2表明存在本原 M-torsion 元素 λ_K，使得 $v_{\infty}(\lambda_K)=\deg M-\frac{q}{q-1}$，即 $v_{\mathscr{P}}(\lambda_K)=(q-1)(\deg M-1)-1$. 根据定理1.2.2的证明有以下引理：

引理1.2.3 对每个 $A \in R, \deg A < \deg M$，则

$$v_{\mathscr{P}}(\lambda_K^A) = (q-1)(\deg M - \deg A - 1) - 1.$$

特别地，存在本原 M-torsion 元素 λ，使得 $v_{\mathscr{P}}(\lambda)=-1$.

证明 第一个推断见定理1.2.2的证明. 第二个论断是由于存在 $A \in R$ 使得 $(A,M)=1, \deg A=\deg M-1$. ▌

定理1.2.4 设 λ 是本原 M-torsion 元素. 则 $K^+=k(\lambda^{q-1})$ 是分圆函数域 $K=k(\Lambda_M)=k(\lambda)$ 对于 ∞ 的分解域（由于 $f=1$，从而 K^+ 是 ∞ 在 K 中的最大不分歧子域）. 并且分解群 $\mathrm{Gal}(K/K^+)$ 为 $J=\{\sigma_a : a \in \mathbf{F}_q^*\}$.

证明 以 $\mathscr{P}$ 表示 ∞ 到 K 的一个扩充素除子，K^+ 是 ∞ 在 K 中的分解域，则 ∞ 在 K 中的分解群为：

$$J = \{\sigma_A : (A,M) = 1, \deg A < \deg M, \sigma_A(\mathscr{P}) = \mathscr{P}\},$$

并且 $|J|=[K:K^+]=e=q-1$. 如果 $\sigma_A \in J$，则 $\sigma_A(\mathscr{P})=\mathscr{P}$，所以 $\sigma_A^{-1}(\mathscr{P})=\mathscr{P}$. 于是由引理1.2.3，得

$$\begin{aligned}(q-1)(\deg M-1)-1 &= v_{\mathscr{P}}(\lambda_K) = v_{\sigma_A^{-1}(\mathscr{P})}(\lambda_K) \\ &= v_{\mathscr{P}}(\sigma_A(\lambda_K)) = v_{\mathscr{P}}(\lambda_K^A) \\ &= (q-1)(\deg M - \deg A - 1) - 1,\end{aligned}$$

这就表明 $\deg A=0$，即 $A \in \mathbf{F}_q^*$. 所以 $J=\{\sigma_a : a \in \mathbf{F}_q^*\}$.

再证 $K^+=k(\lambda^{q-1})$. 对每个 $a \in \mathbf{F}_q^*$，

$$\sigma_a(\lambda^{q-1}) = \sigma_a(\lambda)^{q-1} = (a\lambda)^{q-1} = \lambda^{q-1}.$$

这就表明 $K^+ \supseteq k(\lambda^{q-1})$. 另一方面，$\lambda$ 在 k 上的极小多项式为：

$$\begin{aligned} f(u) &= \prod_{A\in (R/(M))^*} (u - \lambda^A) \\ &= \prod_{A\in (R/(M))^*/F_q^*} \prod_{a\in F_q^*} (u - a\lambda^A) \\ &= \prod_{A\in (R/(M))^*/F_q^*} (u^{q-1} - (\lambda^A)^{q-1}). \end{aligned}$$

所以 $f(u)$ 是 u^{q-1} 的多项式. 设 $f(u)=g(u^{q-1})$，则 $g(u)$ 就是 λ^{q-1} 在 k 上的极小多项式，而

$$\deg g(u) = \frac{\deg f(u)}{q-1} = \frac{\Phi(M)}{q-1}.$$

于是

$$\begin{aligned} q-1 = [K:K^+] \geqslant [K:k(\lambda^{q-1})] &= \frac{[K:k]}{[k(\lambda^{q-1}):k]} \\ &= \frac{\Phi(M)}{\deg g(u)} = q-1. \end{aligned}$$

所以 $K^+ = k(\lambda^{q-1})$. ▌

根据定理1.2.4，k 的无限素除子 ∞ 在 K^+ 中分解成 $\frac{\Phi(M)}{q-1}=g$ 个无限素除子的乘积为：

$$\infty = \mathscr{P}_1^+ \mathscr{P}_2^+ \cdots \mathscr{P}_g^+,$$

面每个 $\mathscr{P}_i^+$ 在 $K=k(\Lambda_M)$ 中完全分歧：$\mathscr{P}_i^+ = \mathscr{P}_i^{q-1}$ $(1\leqslant i\leqslant g)$. 对于数域情形，有理数域 $\boldsymbol{Q}$ 的无限素除子在代数数域 K 中的最大不分歧子域就是 K 的最大实子域 $K^+ = K\cap \boldsymbol{R}$（其中 $\boldsymbol{R}$ 表示实数域）. 例如分圆数域 $\boldsymbol{Q}(\zeta_m)$ $(\zeta_m = e^{\frac{2\pi i}{m}})$ 的最大实子域为 $\boldsymbol{Q}(\zeta_m+\zeta_m^{-1})$. 类比之下有如下的定义：

定义1.2.5 域 $K^+ = k(\lambda^{q-1})$ 称作分圆函数域 $K=k(\Lambda_M)=k(\lambda)$ 的最大"实"子域.

本节最后讨论分圆函数域的单位群. 一般地，设 K 是以 $\boldsymbol{F}_q$ 为常数域的任意函数域，则总存在 $T\in K$，使得 K 是有理函数域

$k=\boldsymbol{F}_q(T)$的有限可分扩张. K 的整数环 O_K 即指 $\boldsymbol{R}=\boldsymbol{F}_q[T]$在 K 中的整闭包,而环 O_K 的单位群(有时也称作 K 的单位群)表示成 U_K. 熟知这是有限生成阿贝尔群,它的 torsion 部分为 $\boldsymbol{F}_q^*$,而自由部分的秩 r 等于$\infty=\left(\frac{1}{T}\right)$在 K 中扩充素除子的个数减1,于是

$$U_K = \boldsymbol{F}_q^* \times V_K \quad (\text{直积}),$$

其中 V_K 是秩 r 的自由阿贝尔群. V_K 的每组基都称作 K 的一个*基本单位系*. 一般来说,寻求 K 的基本单位系是一个重要而又困难的课题.

对于分圆函数域 $K=k(\Lambda_M)$,我们以 U_K 和 U_K^+ 分别表示 K 和 K^+的单位群,则 U_K^+ 是 U_K 的子群. 由于$\infty=\left(\frac{1}{T}\right)$在 K 和 K^+中的扩充素除子的个数均为 $s=\dfrac{\Phi(M)}{q-1}$. 从而 U_K 和 U_K^+ 有同样的 torsion 部分 $\boldsymbol{F}_q^*$,并且自由部分的秩均为 s,所以

$$Q = [U_K:U_K^+]$$

是有限的. 为了以后的需要,下面计算 Q 的值.

引理1.2.6　设 $K=k(\Lambda_M)$,$k=\boldsymbol{F}_q(T)$. 则当 $M=P^n$ 时(其中 $n\geqslant1$,P 是 $R=\boldsymbol{F}_q[T]$中首1不可约多项式),则 $Q=1$. 否则,$Q=q-1$.

证明　$J=\{\sigma_a;a\in\boldsymbol{F}_q^*\}$是$\infty$在 K 中的分解群,所以对 K 的每个无限素除子 $\mathscr{P}$,$\sigma_a(\mathscr{P})=\mathscr{P}(a\in\boldsymbol{F}_q^*)$. 现在令 g 是乘法循环群 $\boldsymbol{F}_q^*$ 的生成元,则 J 是由 σ_g 生成的 $q-1$阶循环群. 而对每个 $\varepsilon\in U_K$ 和 K 的每个无限素除子 $\mathscr{P}$,有

$$\begin{aligned} v_{\mathscr{P}}\left(\frac{\sigma_g(\varepsilon)}{\varepsilon}\right) &= v_{\mathscr{P}}(\sigma_g(\varepsilon)) - v_{\mathscr{P}}(\varepsilon) = v_{\sigma_g^{-1}(\mathscr{P})}(\varepsilon) - v_{\mathscr{P}}(\varepsilon) \\ &= v_{\mathscr{P}}(\varepsilon) - v_{\mathscr{P}}(\varepsilon) = 0, \end{aligned}$$

而对 K 的每个有限素除子 $\mathscr{P}$,由于 $\varepsilon\in U_K$,可知也有

$$v_{\mathscr{P}}\left(\frac{\sigma_g(\varepsilon)}{\varepsilon}\right) = 0 - 0 = 0.$$

这表明$\dfrac{\sigma_g(\varepsilon)}{\varepsilon}\in\boldsymbol{F}_q^*$. 所以我们有群同态:

$$\varphi: U_K \to \boldsymbol{F}_q^*, \quad \varphi(\varepsilon) = \frac{\sigma_K(\varepsilon)}{\varepsilon}.$$

由于

$$\varepsilon \in \mathrm{Ker}\varphi \Longleftrightarrow \sigma_K(\varepsilon) = \varepsilon \Longleftrightarrow \varepsilon \in K^+ \cap U_K = U_K^+,$$

可知 $\mathrm{Ker}\varphi = U_K^+$. 于是有群的单同态 $U_K/U_K^+ \to \boldsymbol{F}_q^*$, 并且

$$Q = [U_K : U_K^+] = |I_m\varphi|.$$

现在设 $M=P^n$. 由于 P 在 K 中完全分歧, 从而在 K^+ 中也完全分歧. 设 $\mathscr{P}^+$ 是 P 在 K^+ 中的唯一扩充, 则对每个 $\varepsilon \in U_K$, $\mathscr{P}^+$ 在 $K^+(\varepsilon)$ 中也完全分歧. 另一方面, 由 $\varphi(\varepsilon^{q-1})=1$ 可知 $\varepsilon^{q-1} \in U_K^+$, 而 ε 是 $x^{q-1}-\varepsilon^{q-1} \in K^+[x]$ 的根. 由于 $x^{q-1}-\varepsilon^{q-1}$ (mod $\mathscr{P}^+$) 没有重根, 可知 $\mathscr{P}^+$ 在 $K^+(\varepsilon)$ 中不分歧. 这表明 $K^+(\varepsilon)=K^+$, 即 $\varepsilon \in K^+ \cap U_K = U_K^+$. 从而 $U_K = U_K^+$, 即 $Q=1$.

现在设 $M=\prod_{i=1}^{g} P_i^{e_i}$, 其中 $g \geqslant 2$, 而 $P_1, \cdots, P_g$ 是 R 中不同的首1不可约多项式, $e_i \geqslant 1$ $(1 \leqslant i \leqslant g)$. 令 λ 是本原 M-torsion 元素. 我们先证 $\lambda \in U_K$. 为方便起见, 以 Λ_M^* 表示所有本原 M-torsion 元素构成的集合. 则 λ 在 k 上的极小多项式为

$$f_M(u) = \prod_{\mu \in \Lambda_M^*} (u-\mu).$$

于是 $N_{K/k}(\mu) = \pm f_M(0)$. 另一方面,

$$u^M = \prod_{\alpha \in \Lambda_M} (u-\alpha) = \prod_{N|M} \prod_{\alpha \in \Lambda_N^*} (u-\alpha) = \prod_{N|M} f_N(u),$$

其中 N 过 M 的所有首1多项式的因子, 利用 Möbius 变换可知

$$f_M(u) = \prod_{N|M} (u^{M/N})^{\mu(N)},$$

其中 $\mu(M)$ 是如下定义的函数: 对于 R 中每个首1多项式 M,

$$\mu(M) = \begin{cases} 1, & \text{若 } M = 1; \\ (-1)^t, & \text{若 } M \text{ 是 } t \text{ 个不同的首 1 不可约多项式之积}; \\ 0, & \text{否则}. \end{cases}$$

与通常的 Möbius 函数一样, 可知当 $\deg M \geqslant 1$ 时, $\sum_{N|M} \mu(N) = 0$, 于是

$$f_M(u) = \prod_{N|M}\left(\frac{u^{M/N}}{u}\right)^{\mu(N)}.$$

由于多项式 u^N 对于 u 的最低次项为 Nu，于是

$$\begin{aligned}f_M(0) &= \prod_{N|M}\left(\frac{M}{N}\right)^{\mu(N)} = \prod_{N|M} N^{-\mu(N)} \\ &= \prod_{i_1=0}^{1}\cdots\prod_{i_g=0}^{1}(P_1^{i_1}\cdots P_g^{i_g})^{-\mu(P_1^{i_1}\cdots P_g^{i_g})} \\ &= P_1^{r_1}\cdots P_g^{r_g},\end{aligned}$$

其中(注意 $g\geqslant 2$)

$$r_1 = -\sum_{i_1=0}^{1}\cdots\sum_{i_g=0}^{1}\mu(P_1^{i_1})\cdots\mu(P_g^{i_g}) = 0.$$

因为 $\sum_{i=0}^{1}\mu(P^i)=1-1=0$. 类似可知 $r_2=\cdots=r_g=0$. 于是 $N_{K/k}(\lambda)=\pm f_M(0)=\pm 1$. 这表明了 $\lambda\in U_K$.

由于 $1,\lambda,\cdots,\lambda^{q-2}$ 是 $K^+=k(\lambda^{q-1})$ 上向量空间 $K=k(\lambda)$ 的一组基，知每个 $\varepsilon\in U_K$ 可唯一地表示成

$$\varepsilon = \sum_{i=0}^{q-2} a_i\lambda^i, a_i \in K^+.$$

由于
$$b=\sigma_g(\varepsilon)/\varepsilon\in \boldsymbol{F}_q^*,$$

可知
$$b\varepsilon=\sigma_g(\varepsilon)=\sum_{i=0}^{q-2}a_i g^i\lambda^i.$$

因此 $ba_i=a_i g^i(0\leqslant i\leqslant q-2)$. 所以必有唯一的 i，使得 $a_i\neq 0, b=g^i$，而当 $j\neq i$ 时，$a_j=0$. 于是 $\varepsilon=a_i\lambda^i$，而 $a_i\in K^+\cap U_K=U_K^+$. 由于 $\lambda^i(1\leqslant i\leqslant q-2)$ 均不属于 U_K^+，这表明 U_K 对 U_K^+ 有 $q-1$ 个陪集 $\lambda^i U_K^+(0\leqslant i\leqslant q-2)$，于是 $Q=[U_K:U_K^+]=q-1$. 引理证毕. ▮

§1.3　除子类群和理想类群

设 K 是 $k=\boldsymbol{F}_q(T)$ 的有限扩域，并且 K 的常数域为 $\boldsymbol{F}_q$. 我们以 $S_\infty=S_\infty(K)$ 表示 K 的无限素除子集合；$S_f=S_f(K)$ 表示 K 的

有限素除子集合，而$S=S_\infty\cup S_f$是K的素除子集合. 对于每个$\mathscr{P}\in S$，以$v_{\mathscr{P}}$表示K的$\mathscr{P}$-adic标准指数赋值，$v_{\mathscr{P}}(K^*)=\mathbf{Z}$. $O_{\mathscr{P}}=\{\alpha\in K;v_{\mathscr{P}}(\alpha)\geqslant 0\}$为局部域$K_{\mathscr{P}}$的整数环，而局部环$O_{\mathscr{P}}$的唯一极大理想仍记为$\mathscr{P}$. 则$\overline{K}_{\mathscr{P}}=O_{\mathscr{P}}/\mathscr{P}$是$\mathbf{F}_q$的有限扩张. $[\overline{K}_{\mathscr{P}}:\mathbf{F}_q]$称作素除子$\mathscr{P}$的次数，表示成$\deg\mathscr{P}$. 特别对$K=k$的情形，对于$k$的有限素除子$P$，这里所定义的$\deg P$和多项式$P$的次数是一致的. 而对$k$的无限素除子$\infty$，$\deg\infty=1$. 一般地，设$K$的素除子$\mathscr{P}$是$k$中素除子$P$的扩充，以$f(\mathscr{P}/P)$表示$\mathscr{P}$对于$P$的剩余类域的次数，即$f(\mathscr{P}/P)=[\overline{K}_{\mathscr{P}}:\bar{k}_P]$，则

$$\deg\mathscr{P}=[\overline{K}_{\mathscr{P}}:\mathbf{F}_q]=[\overline{K}_{\mathscr{P}}:\bar{k}_P][\bar{k}_P:\mathbf{F}_q]=f(\mathscr{P}/P)\deg P.$$

以K的所有素除子为基作成的自由阿贝尔群称作K的除子群，表示成$D(K)$. 其中每个元素可唯一地表示成：

$$\mathfrak{A}=\prod_{\mathscr{P}\in S(K)}\mathscr{P}^{n_{\mathscr{P}}}(\text{有限乘积})\quad(n_{\mathscr{P}}\in\mathbf{Z}),$$

称作K的一个除子. 而除子$\mathfrak{A}$的次数定义为

$$\deg\mathfrak{A}=\sum_{\mathscr{P}}n_{\mathscr{P}}\deg\mathscr{P}.$$

映射 $\deg:D(K)\to\mathbf{Z}$ (整数加法群)

是群的同态. 可以证明这是满同态(即K中存在一次除子)，核$D^0(K)=\ker(\deg)$是$D(K)$的零次除子构成的子群. 进而，对每个元素$\alpha\in K^*$，可以定义一个除子

$$\operatorname{div}(\alpha)=\prod_{\mathscr{P}}\mathscr{P}^{v_{\mathscr{P}}(\alpha)},$$

称为主除子. 可以证明$\deg(\operatorname{div}(\alpha))=0$，于是有群同态

$$\operatorname{div}:K^*\to D^0(K),$$

它的核为$\mathbf{F}_q^*$. 商群

$$C(K)=\frac{D(K)}{\operatorname{div}(K^*)}\text{ 和 }C^0(K)=\frac{D^0(K)}{\operatorname{div}(K^*)}$$

分别称作K的除子类群和零次除子类群，而$C(K)$中的元素称为K的一个除子类. 每个除子类中的除子都有相同的次数，我们就称它为这个除子类的次数. 利用 Riemann-Roch 定理可以证明

$C^0(K)$是有限阿贝尔群，它的阶 $h(K)=|C^0(K)|$称作 K 的(零次)除子类数.

K 的每个有限素除子是 O_K 的极大理想(即非零素理想)，由 K 的所有有限素除子为基，构成的自由阿贝尔群，就是 K 的分式理想群，表示成 $D(O_K)$，它是 $D(K)$的子群. 而主分式理想的全体

$$P(O_K) = \{(\alpha) = \alpha O_K : \alpha \in K^*\}$$

是 $D(O_K)$的子群. 商群

$$C(O_K) = \frac{D(O_K)}{P(O_K)}$$

也是有限阿贝尔群，称作 O_K(或 K)的**理想类群**，它的阶 $h(O_K)=|C(O_K)|$称作 O_K(或 K)的**理想类数**.

以 K 的所有无限素除子为基构成的自由阿贝尔群记为 $D_\infty(K)$. 令

$$D_\infty^0(K) = D_\infty(K) \cap D^0(K),$$

则 $\mathrm{div}(U_K)$是 $D_\infty^0(K)$的子群. 令 e 为 K 的所有有限素除子次数的最大公因子；d 为 K 的所有无限素除子次数的最大公因子. 我们有群的正合序列

$$0 \to \frac{D_\infty^0(K)}{\mathrm{div}(U_K)} \xrightarrow{g} C^0(K) = \frac{D^0(K)}{\mathrm{div}(K^*)} \xrightarrow{f} C(O_K)$$

$$= \frac{D(O_K)}{P(O_K)} \xrightarrow{\deg} \frac{e\mathbf{Z}}{[e,d]\mathbf{Z}} \to 0,$$

其中 g 为自然嵌入(因为 $\mathrm{div}(U_K)=D_\infty^0(K)\cap\mathrm{div}(K^*)$)，$f$ 为“忘掉无限部分”，群 $D_\infty^0(K)/\mathrm{div}(U_K)$的阶称作 O_K(或 K)的 regulator，表示成

$$R(O_K) = \left|\frac{D_\infty^0(K)}{\mathrm{div}(U_K)}\right|.$$

所以由上面正合序列得到

$$R(O_K)h(O_K) = h(K)\frac{[e,d]}{e} = h(K)\frac{d}{(e,d)},$$

可以证明$(e,d)=1$(这等价于 K 中存在1次除子)，于是最后得到

$$R(O_K)h(O_K) = h(K)d, \qquad (1.3.1)$$

其中 d 是 K 的所有无限素除子次数的最大公因子.

对于分圆函数域 $K=k(\Lambda_M)$, K 的每个无限素除子 $\mathscr{P}$ 的次数均为

$$\deg\mathscr{P} = f(\mathscr{P}/\infty)\deg\infty = 1 \quad (\text{定理 } 1.2.2),$$

于是 $d=1$, 即 $h(K)=h(O_K)R(O_K)$. 对于 K 的任何子域 $L(\geqslant k)$, L 中的无限素除子也都是1次的, 所以也都有 $h(L)=h(O_L)\times R(O_L)$.

现在我们给出 $R(O_K)$ 的另一个表达式, 可看出它与数域的 regulator 很相像.

引理1.3.1 设 $k=\boldsymbol{F}_q(T)$, K/k 是有限扩张, $s=|S_\infty(K)|$ 为 K 中无限素除子的个数, $r=s-1$. 令 $\mathscr{P}_1,\cdots,\mathscr{P}_s$ 是 K 的全部无限素除子, $\varepsilon_1,\cdots,\varepsilon_r$ 是 K 的一组基本单位系. 则

$$R(O_K) = \det(v_{\mathscr{P}_i}(\varepsilon_j)_{1\leqslant i,j\leqslant r}) \text{ 的绝对值.}$$

证明 令 $d_i=\deg\mathscr{P}_i(1\leqslant i\leqslant s)$. 又记 $\bar{e}_1,\cdots,\bar{e}_s$ 是实向量空间 $\boldsymbol{R}^s$ 的标准基, 其中 $\bar{e}_i$ 的第 i 个坐标为1, 而其余坐标为零. 考虑群的单同态

$$l: D_\infty^0(K) \to \boldsymbol{R}^s,$$

$$l(\mathfrak{a}) = (d_1v_{\mathscr{P}_1}(\mathfrak{a}),\cdots,d_sv_{\mathscr{P}_s}(\mathfrak{a})) = \sum_{i=1}^{s} d_iv_{\mathscr{P}_i}(\mathfrak{a})\bar{e}_i.$$

则象集合 $\mathrm{Im}(l)$ 包含在 $\boldsymbol{R}^s$ 的超平面

$$H = \{(a_1,\cdots,a_s)\in\boldsymbol{R}^s: a_1+a_2+\cdots+a_s=0\}$$

之中. 注意 $\boldsymbol{R}^s=H\oplus\bar{e}_s\boldsymbol{R}$, 于是

$$\begin{aligned} R(O_K) &= [D_\infty^0(K):\mathrm{div}(U_K)] \\ &= [l(D_\infty^0(K)):l(\mathrm{div}(U_K))] \\ &= [d_sl(D_\infty^0(K))+\bar{e}_s\boldsymbol{Z}:d_sl(\mathrm{div}(U_K))+\bar{e}_s\boldsymbol{Z}]. \end{aligned}$$

上式右端两个集合均为 $\boldsymbol{R}^s$ 中秩 s 的格. 前者 $L'=d_sl(D_\infty^0(K))+\bar{e}_s\boldsymbol{Z}$ 有 $\boldsymbol{Z}$-基 $d_sd_i\bar{e}_i(1\leqslant i\leqslant r)$ 和 $\bar{e}_s$; 后者 $L=d_sl(\mathrm{div}(U_K))+\bar{e}_s\boldsymbol{Z}$ 有 $\boldsymbol{Z}$-基 $\bar{e}_s$ 和

$$d_t l(\varepsilon_j) = d_t \sum_{i=1}^{s} v_{\mathscr{P}_i}(\varepsilon_j) d_i \tilde{e}_i \quad (1 \leqslant j \leqslant r).$$

于是

$$\begin{aligned}
R(O_K) &= [L' : L] \\
&= \det \begin{pmatrix} v_{\mathscr{P}_1}(\varepsilon_1), & \cdots, & v_{\mathscr{P}_r}(\varepsilon_1), & d_i^2 v_{\mathscr{P}_i}(\varepsilon_1) \\ \cdots & \cdots & \cdots & \cdots \\ v_{\mathscr{P}_1}(\varepsilon_r), & \cdots, & v_{\mathscr{P}_r}(\varepsilon_r), & d_i^2 v_{\mathscr{P}_i}(\varepsilon_r) \\ 0, & \cdots, & 0, & 1 \end{pmatrix} \text{的绝对值} \\
&= \det\left(v_{\mathscr{P}_i}(\varepsilon_j)_{1 \leqslant i,j \leqslant r} \right) \text{的绝对值}.
\end{aligned}$$

这就证明了引理1.3.1. ∎

引理1.3.2 设 $k = \boldsymbol{F}_q(T)$，$K = k(\Lambda_M)$，$r = \dfrac{\Phi(M)}{q-1} - 1$. 以 $R(O_K^+)$表示 K^+的 regulator，则

$$\frac{R(O_K)}{R(O_K^+)} = \begin{cases} (q-1)^r, & \text{若 } M = P^n; \\ (q-1)^{r-1}, & \text{否则}. \end{cases}$$

证明 以 $\mathscr{P}_i^+$ 和 $\mathscr{P}_i(1 \leqslant i \leqslant r+1)$分别表示 K 和 K^+的无限素除子，$\mathscr{P}_i^+ = \mathscr{P}_i^{q-1}$. 又令$\{\varepsilon_1^+, \cdots, \varepsilon_r^+\}$和$\{\varepsilon_1, \cdots, \varepsilon_r\}$分别是 K^+和 K 的基本单位系. 由 $U_K^+ \subseteq U_K$ 可知

$$\varepsilon_i^+ = \prod_{j=1}^{r} \varepsilon_j^{a_{ij}}, a_{ij} \in \mathbf{Z}.$$

由于 U_K^+ 和 U_K 的 torsion 部分都是 $\boldsymbol{F}_q^*$，因此

$$[U_K : U_K^+] = |\det(a_{ij})|.$$

但是引理1.2.6已经算出

$$[U_K : U_K^+] = Q = \begin{cases} 1, & \text{若 } M = P^n; \\ q-1, & \text{否则}. \end{cases}$$

再由 $v_{\mathscr{P}_i}(\varepsilon_j^+) = (q-1) v_{\mathscr{P}_i^+}(\varepsilon_j^+)$便得到

$$\begin{aligned}
R(O_K^+) &= |\det(v_{\mathscr{P}_i^+}(\varepsilon_j^+))_{1 \leqslant i,j \leqslant r}| \\
&= (q-1)^{-r} |\det(v_{\mathscr{P}_i}(\varepsilon_j^+))| \\
&= (q-1)^{-r} |\det(v_{\mathscr{P}_i}(\varepsilon_j))| \cdot |\det(a_{ij})| \\
&= (q-1)^{-r} Q\, R(O_K)
\end{aligned}$$

由此即得引理. ▌

§1.4 阿贝尔函数域

每个分圆函数域 $k(\Lambda_M)$ 的子域都是 $k=\boldsymbol{F}_q(T)$ 的阿贝尔扩域，所以

$$K_T=\bigcup_M k(\Lambda_M)$$

是 k 的(无限)阿贝尔扩域，其中 M 过 $R=\boldsymbol{F}_q[T]$ 中所有首1多项式. 这个域依赖于 k 中超越元素 T 的选取. 如果取 T^{-1} 为新的超越元素，则可类似地得到 k 的阿贝尔扩域 $K_{T^{-1}}$. 此外，k 的常数域扩张 $k\boldsymbol{F}_{q^\infty}=\boldsymbol{F}_{q^\infty}(T)$ 也是 k 的阿贝尔扩域，其中 $\boldsymbol{F}_{q^\infty}=\bigcup_{n\geq 1}\boldsymbol{F}_{q^n}$. 1974 年，D. Hayes[39] 利用类域论证明了这三个域的合成

$$k^{ab}=K_TK_{T^{-1}}\boldsymbol{F}_{q^\infty}$$

就是 k 的最大阿贝尔扩域，也即 k 的每个阿贝尔扩域都是 k^{ab} 的子域. 所以在研究 k 的阿贝尔扩张时，分圆函数域的子域起着基本的作用.

在本书中，我们把分圆函数域 $k(\Lambda_M)$ 的子域 $K(\supseteq k)$ 称作阿贝尔函数域，而满足 $K\subseteq k(\Lambda_M)$ 的次数最小首1多项式 M 称作阿贝尔域 K 的导子，表示成 $\mathrm{Cond}(K)$.

今后我们常把 $k(\Lambda_M)/k$ 的伽罗华群

$$G=\{\sigma_A:A\in(R/(M))^*\}$$

等同于 $(R/(M))^*$. 从而有限阿贝尔群 G 的特征 χ(即 χ 是 G 到乘法群 $\boldsymbol{C}^*$ 的同态)也看成是群 $(R/(M))^*$ 的特征：$\chi(\sigma_A)=\chi(A)$. 当 $(A,M)\neq 1$ 时，规定 $\chi(A)=0$. 类比与 $\boldsymbol{Z}/m\boldsymbol{Z}$ 的情形，我们也把 $(R/(M))^*$ 的特征称作 R 的模 M 的 Dirichlet 特征，或简称模 M 特征.

设 χ 是 $R=\boldsymbol{F}_q[T]$ 上模 M 特征. 如果 M 存在首1多项式因子 N，$\deg N<\deg M$，并且有模 N 特征 χ'，使得当 $A\in R$，$(A,M)=1$ 时，$\chi(A)=\chi'(A)$，则称 χ 是由 χ' 诱导的，并且这时 χ 称作是非本

原特征. 否则,χ 称为本原特征. 同 $\mathbf{Z}/m\mathbf{Z}$ 的情形一样,R 上模 M 的每个特征 χ 都是由唯一的模 N 本原特征 χ^* 所诱导的,我们称 N 为特征 χ 的导子,表示成 $\mathrm{Cond}(\chi)$ 或 F_χ. 而 χ^* 称作与 χ 相结合的本原特征. 当 χ 是模 M 本原特征时,令 $F_\chi=M$, $\chi^*=\chi$. 最后,我们以 χ_0 表示模 M 的平凡特征,即对每个 $A\in R$,当 $(A,M)=1$ 时 $\chi_0(A)=1$,否则,$\chi_0(A)=0$. 于是 $F_{\chi_0}=1$.

现在设 K 为阿贝尔函数域,$K\subseteq k(\Lambda_M)$,则在伽罗华对应下,K 对应于 $\mathrm{Gal}(k(\Lambda_M)/k)=(R/(M))^*$ 的子群

$$\begin{aligned}E_K&=\{A\in(R/(M))^*:\sigma_A(\alpha)=\alpha\ \text{对每个}\ \alpha\in K\}\\&=\mathrm{Gal}(k(\Lambda_M)/K).\end{aligned}$$

于是 $\mathrm{Gal}(K/k)\cong(R/(M))^*/E_K$,从而 $\mathrm{Gal}(K/k)$ 的每个特征可看成是 R 上满足 $\chi(E_K)=1$ 的模 M 特征. 今后我们把 $\mathrm{Gal}(K/k)$ 的特征群也常称为是 K 的特征群,并且表示为 $\hat{K}$. 若 $k\subseteq L\subseteq K$,则 $E_K\subseteq E_L$,从而 $\hat{L}\subseteq\hat{K}$. 所以对应 $L\rightarrow\hat{L}$ 是保序的.

$$\begin{array}{ccc}k(\Lambda_M) & \qquad & \{1\}\\ | & & |\\ K & & E_K\\ | & & |\\ k & & (R/(M))^*\end{array}$$

设 $M=\prod_P P^{e_P}$ 是 M 的分解式,则

$$(R/(M))^*\cong\prod_P(R/(P^{e_P}))^*\ (\text{直积}).$$

所以 R 上每个模 M 特征可唯一地表示成

$$\chi=\prod_P\chi_P,$$

其中 χ_P 是模 P^{e_P} 特征. 易知 $F_\chi=\prod_P F_{\chi_P}$. 对于阿贝尔函数域 $K\subseteq k(\Lambda_M)$,记 $X=\hat{K}$ 为 K 的特征群. 对每个首1不可约多项式 P,令

$$\begin{aligned}&X_P=\{\chi_P:\chi\in X\},Y=\{\chi\in X:\chi^*(P)\neq 0\},\\&Z=\{\chi\in Y:\chi^*(P)=1\}.\end{aligned}$$

我们可以用 X_P 和 X 的子群 Y 和 Z 来刻划 P 在 K 中的分解情形.

定理1.4.1　以 e、f、g 分别表示 P 在阿贝尔函数域 $K(\subseteq k(\Lambda_M))$ 中的分歧指数、剩余类域次数和分解次数,则

(1) $e=|X_P|$,并且 P 在 K 中分歧的充分必要条件是:存在 $\chi\in X$,使得 $\chi^*(P)=0$ (即 $P|F_\chi$).

(2) Y 和 Z 分别是 K 的惰性域和分解域的特征群. 于是

$$e=[X:Y],\ f=[Y:Z],\ g=|Z|.$$

证明 (1) 设 $M=P^nN,(P,N)=1,n\geqslant 0$,我们有如下的域扩张图表如图1.1. 图中每个域的特征群均看成是 $k(\Lambda_M)$ 的特征群 $((R/(M))^*)^\wedge$ 的子群. 由于 $L=K(\Lambda_N)$ 是 $k(\Lambda_N)$ 和 K 的合成,可知 $\hat{L}$ 是由 $k(\Lambda_N)^\wedge$ 和 $\hat{K}=X$ 生成的特征群,即

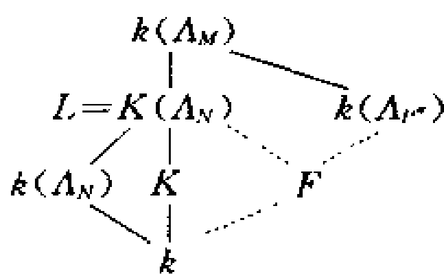


图 1.1

$$\hat{L}=\langle((R/(N))^*)^\wedge,X\rangle=((R/(N))^*)^\wedge\times X_P(\text{直积}).$$

于是 $L=k(\Lambda_N)\cdot F$,其中 $F\subseteq k(\Lambda_{P^n})$,$\hat{F}=X_P$(见图1.1中虚线所示). 对于 $k(\Lambda_M)$ 的每个子域 W,用 $e(W)$ 表示 P 在 W 中的分歧指数,则

$$\begin{aligned}e=e(K)&=e(L)\quad(\text{由于 } e(k(\Lambda_N))=1,\ L=k(\Lambda_N)K)\\&=e(F)\quad(\text{由于 } L=k(\Lambda_N)F,\ e(k(\Lambda_N))=1)\\&=[F:k]\quad(\text{由于 } F\subseteq k(\Lambda_{P^n}),\text{从而 } P \text{ 在 } F \text{ 中完全分歧})\\&=\hat{F}=|X_P|.\end{aligned}$$

进而,P 在 K 中分歧 $\Leftrightarrow|X_P|=e\geqslant 2\Leftrightarrow$ 存在 $\chi\in X$,使得 $\chi_P\neq\chi_0\Leftrightarrow$ 存在 $\chi\in X$ 使得 $\chi^*(P)=0$. 这就证明了(1).

(2) 设 W 为 K 的任一子域. 由(1)知:

P 在 W 中不分歧 $\Leftrightarrow$ 对每个 $\chi\in\hat{W}$,均有 $\chi^*(P)\neq 0\Leftrightarrow\hat{W}\subseteq Y$. 这就表明 Y 对应着 P 在 K 中的最大不分歧子域 K_I(即惰性域). 于是

$$Y=\hat{K}_I,e=[K:K_I]=[\hat{K}:\hat{K}_I]=[X:Y].$$

进而对每个 $\chi\in Y$,由 $\chi^*(P)\neq 0$ 可知 $F_\chi|N$. 所以 χ 是由一个确定的模 N 特征 χ' 所诱导的,并且 $(\chi')^*=\chi^*$. 另一方面,$k(\Lambda_N)$ 是 P 在 $k(\Lambda_M)$ 中的最大不分歧子域,于是 $K_I\subseteq k(\Lambda_N)$. 以 K_D 表示 P 在

K 中的分解域，则有图1.2所示. 其中 I 和 D 是 $(R/(N))^*$ 的子群，分别对应于域 K_I 和 K_D. 这时 K_I 的特征群 $((R/(N))^*)^\wedge$ 就是 $Y'=\{\chi':\chi\in Y\}$. 由于

$$\mathrm{Gal}(K_D/k)=(R/(N))^*/D\cong\frac{(R/(N))^*/I}{D/I},$$

所以对每个 $\chi'\in Y'=((R/(N))^*/I)^\wedge$：

χ' 为 $\mathrm{Gal}(K_D/k)$ 的特征 $\Leftrightarrow\chi'(D/I)=1$

$\Leftrightarrow\chi'(P)=1$ （因为 D/I 是由 σ_P 生成的循环群）

$\Leftrightarrow\chi^*(P)=1\Leftrightarrow\chi\in Z$.

于是 $\hat{K}_D=Z$，从而 $f=[K_I:K_D]=[Y:Z]$，$g=|Z|$. 定理得证. ▌

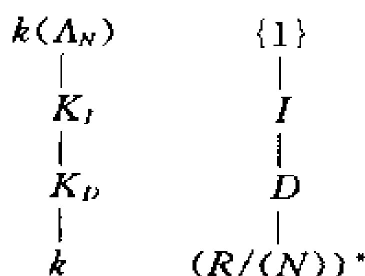


图　1.2

类似地可讨论 k 的无限素除子 $\infty=\left(\frac{1}{T}\right)$ 在阿贝尔函数域 $K(\subseteq k(\Lambda_M))$ 中的分解. 由于 ∞ 在 $k(\Lambda_M)$ 中的最大不分歧子域为 $k(\Lambda_M)^+$，于是 ∞ 在 K 中的最大不分歧子域（惰性域）为 $K^+=K\cap k(\Lambda_M)^+$. 我们把 K^+ 称作 K 的最大实子域，它也是 ∞ 在 K 中的分解域（由于 $f=1$）. 定理1.2.4给出如下的伽罗华对应图表（图1.3）.

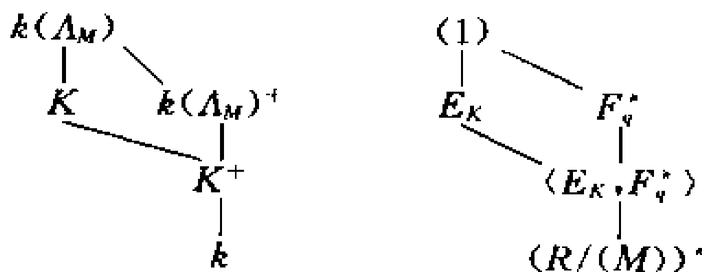


图　1.3

现在引入如下定义：

定义1.4.2　R 上模 M 的特征 χ 称作"实"的，是指 $\chi(F_q^*)=1$；否则，χ 称作非实的.

由于

$$\mathrm{Gal}(k(\Lambda_M)^+/k) = (R/(M))^*/\boldsymbol{F}_q^*,$$

可知 $k(\Lambda_M)^+$的特征群就是由模 M 的所有实特征构成的群. 而对任意的阿贝尔函数域 K,K^+的特征群 $\hat{K}^+$就是 $\hat{K}$中全部实特征构成的子群. ∞在 K 中的分歧指数为:

$$e = [K:K^+] = [\langle E_K, \boldsymbol{F}_q^* \rangle : E_K] = [\boldsymbol{F}_q^* : \boldsymbol{F}_q^* \cap E_K].$$

由定理1.2.4知 $f=1$. 于是

$$g=[K^+:k]=\hat{K}^+=K \text{ 的实特征个数}.$$

我们把上述结果总结成如下定理:

定理1.4.3 设 $k=\boldsymbol{F}_q(T)\subseteq K\subseteq k(\Lambda_M)$,以 e、f、g 表示∞在 K 中的分歧指数、剩余类域次数和分解次数,E_K 是$(R/(M))^*$中对应于域 K 的子群. 则

$$e = [\boldsymbol{F}_q^* : \boldsymbol{F}_q^* \cap E_K], \quad f = 1, eg = [K:k].$$

并且 g 等于 K 的实特征个数(即$[K^+:k]$). ▌

§1.5 类数解析公式

本节给出阿贝尔函数域的类数公式. 为此,需要介绍函数域的 zeta 函数的性质以及它与除子类数的联系.

设 K 是以 $\boldsymbol{F}_q$ 为常数域的函数域,则存在 K 中对 $\boldsymbol{F}_q$ 超越的元素 T,使得 K 是 $k=\boldsymbol{F}_q(T)$的有限可分扩张. 以 $g=g(K)$表示域 K 的亏格(genus),a_n 表示 K 中 n 次整除子的个数(除子 $\mathfrak{a}=\prod_{\mathscr{P}}\mathscr{P}^{n_{\mathscr{P}}}$ 称作整除子,是指对每个 $\mathscr{P}$,$n_{\mathscr{P}}\geqslant 0$). 域 K 的 zeta 函数定义为

$$Z_K(U) = \sum_{n=0}^{\infty} a_n U^n = \sum_{\mathfrak{a}} U^{\deg \mathfrak{a}},$$

其中 $\mathfrak{a}$ 过 K 的所有整除子. A. Weil 的著名定理如下所述:

引理1.5.1 (1) $Z_K(U)=\dfrac{F_K(U)}{(1-U)(1-qU)}$,其中 $F_K(U)\in \mathbf{Z}[U]$,并且 $\deg F_K(U)=2g$;

(2) $h(K)=F_K(1)$;

(3) 函数方程　$Z_K(U)=(\sqrt{q}\,U)^{2g-2}Z_K\left(\dfrac{1}{qU}\right)$.

这也相当于

$$F_K(U)=(\sqrt{q}\,U)^{2g}F_K\left(\frac{1}{qU}\right).$$

由此可推出:若

$$F_K(U)=\sum_{n=0}^{2g}c_nU^n\,(c_n\in\mathbf{C}),$$

则　$c_0=1$, $c_{2g}=q^g$, $c_{2g-n}=q^{g-n}c_n$　$(0\leqslant n\leqslant g)$.

(4) 若 $F_K(U)=\prod\limits_{n=1}^{2g}(1-w_nU)$,其中 $w_n\in\mathbf{C}$,则

$$|w_n|=\sqrt{q}\quad(1\leqslant n\leqslant 2g).\qquad\blacksquare$$

现在利用引理1.5.1计算阿贝尔函数域的 zeta 函数和除子类数公式.

定理1.5.2　设 $k=\mathbf{F}_q(T)$, $k\subseteq K\subseteq k(\Lambda_M)$. 对阿贝尔域 K 的每个特征 χ,我们用 d_χ 表示 χ 的导子 F_χ 的次数. 以 $\hat{K}^-$ 表示 K 的非实特征全体,$\hat{K}^+$ 为 K^+ 的特征群(即 K 的实特征全体). 又以 R_1 表示 R 的首1多项式全体. 定义

$$h(\chi)=\begin{cases}\displaystyle\sum_{\substack{A\in R_1\\0\leqslant\deg A\leqslant d_\chi-1}}\chi^*(A), & \text{若 }\chi\in\hat{K}^-;\\[2ex]\displaystyle-\sum_{\substack{A\in R_1\\1\leqslant\deg A\leqslant d_\chi-1}}\chi^*(A)\deg A, & \text{若 }\chi\in\hat{K}^+.\end{cases}$$

其中 χ^* 表示与 χ 相结合的本原特征. 则

$$h(K)=\prod_{\chi_0\neq\chi\in\hat{K}}h(\chi),\quad h(K^+)=\prod_{\chi_0\neq\chi\in\hat{K}^+}h(\chi).$$

证明　我们先计算 zeta 函数 $Z_K(U)$. 由引理1.5.1(1) 可知,它有欧拉乘积展开

$$\begin{aligned}Z_K(U)&=\sum_{\mathfrak{a}}U^{\deg\mathfrak{a}}=\prod_{\mathfrak{P}\in S(K)}(1-U^{\deg\mathfrak{P}})^{-1}\\&=\prod_{\mathfrak{P}\in S_\infty(K)}(1-U^{\deg\mathfrak{P}})^{-1}\cdot\prod_{\mathfrak{P}\in S_f(K)}(1-U^{\deg\mathfrak{P}})^{-1},\end{aligned}$$

$$(|U|\leqslant q^{-1}).$$

根据定理1.4.3，$\infty=\left(\frac{1}{T}\right)$在$K$中分解成

$$\infty=(\mathscr{P}_1\cdots\mathscr{P}_g)^e.$$

其中$e=[K:K^+]$，$g=[K^+:k]$，$\deg\mathscr{P}_i=1\ (1\leqslant i\leqslant g)$。于是

$$\prod_{\mathscr{P}\in S_\infty(K)}(1-U^{\deg\mathscr{P}})=\prod_{i=1}^{g}(1-U^{\deg\mathscr{P}_i})=(1-U)^g. \tag{1.5.1}$$

而对有限素除子部分，

$$\prod_{\mathscr{P}\in S_f(K)}(1-U^{\deg\mathscr{P}})=\prod_P\prod_{\mathscr{P}|P}(1-U^{\deg\mathscr{P}}),$$

其中P过R中所有首1不可约多项式。我们现在证明：对每个P，有

$$\prod_{\mathscr{P}|P}(1-U^{\deg\mathscr{P}})=\prod_{\chi\in\hat{K}}(1-\chi^*(P)U^{\deg P}). \tag{1.5.2}$$

为证公式(1.5.2)，我们以e'、f'、g'表示P在K中分解的三个参数。则

$$P=(\mathscr{P}_1\cdots\mathscr{P}_g)^{e'},\ \deg\mathscr{P}_i=f'\deg P\quad(1\leqslant i\leqslant g').$$

于是

$$\prod_{\mathscr{P}|P}(1-U^{\deg\mathscr{P}})=(1-U^{f'\deg P})^{g'}. \tag{1.5.3}$$

另一方面，以K_I和K_D分别表示P在K中的惰性域和分解域，对每个$\chi\in\hat{K}$由定理1.4.1知道，在$\chi\notin\hat{K}_I$时，$\chi^*(P)=0$。因此

$$\prod_{\chi\in\hat{K}}(1-\chi^*(P)U^{\deg P})=\prod_{\chi\in\hat{K}_I}(1-\chi^*(P)U^{\deg P}).$$

进而，当$\chi\in\hat{K}_D$时，$\chi^*(P)=1$。从而当$\hat{K}_I$中两个特征χ_1和χ_2属于对子群$\hat{K}_D$的同一陪集时，$\chi_1^*(P)=\chi_2^*(P)$。由于$[\hat{K}_I:\hat{K}_D]=[K_I:K_D]=g'$，可知

$$\prod_{\chi\in\hat{K}}(1-\chi^*(P)U^{\deg P})=\prod_{\chi\in\hat{K}_I/\hat{K}_D}(1-\chi^*(P)U^{\deg P})^{g'}.$$

由定理1.4.1可知群同态

$$\hat{K}_I \to C^*, \quad \chi \mapsto \chi^*(P)$$

的核为 $\hat{K}_D$. 于是我们有单同态 $\hat{K}_I/\hat{K}_D \to C^*$. 但是$[\hat{K}_I:\hat{K}_D]=[K_I:K_D]=f'$,所以像元素 $\chi^*(P)(\chi\in\hat{K}_I/\hat{K}_D)$恰好是 f'个不同的 f'次单位根. 这就表明

$$\prod_{\chi\in\hat{K}_I/\hat{K}_D}(1-\chi^*(P)U^{\deg P})=1-U^{f'\deg P}.$$

于是

$$\prod_{\chi\in\hat{K}}(1-\chi^*(P)U^{\deg P})=(1-U^{f'\deg P})^{g'}. \qquad (1.5.4)$$

由(1.5.3)和(1.5.4)式即得(1.5.2)式.

利用(1.5.1)和(1.5.2)式可得到

$$\begin{aligned}Z_K(U)&=(1-U)^{-g}\prod_{\chi\in\hat{K}}\prod_{P}(1-\chi^*(P)U^{\deg P})^{-1}\\&=(1-U)^{-g}\prod_{\chi\in\hat{K}}L(U,\chi),\end{aligned}$$

其中

$$\begin{aligned}L(U,\chi)&=\prod_{P}(1-\chi^*(P)U^{\deg P})^{-1}=\sum_{A\in R_1}\chi^*(A)U^{\deg A}\\&=\sum_{n=0}^{\infty}\sigma_n(\chi)U^n,\end{aligned} \qquad (1.5.5)$$

式中

$$\sigma_n(\chi)=\sum_{\substack{A\in R_1\\ \deg A=n}}\chi^*(A)$$

对于主特征 χ_0, χ_0^*是 R 上恒取值为1的函数. 于是

$$L(U,\chi_0)=\sum_{A\in R_1}U^{\deg A}=\sum_{n=0}^{\infty}q^nU^n=(1-qU)^{-1}.$$

所以

$$Z_K(U)=(1-U)^{-g}(1-qU)^{-1}\prod_{\substack{\chi\in\hat{K}\\ \chi\neq\chi_0}}L(U,\chi).$$

再由引理1.5.1的(1)可知

$$F_K(U)=(1-U)^{1-\kappa}\prod_{\chi_0\neq\chi\in\hat{K}}L(U,\chi). \qquad (1.5.6)$$

现在证明：当 $\chi\neq\chi_0$ 并且 $n\geqslant d_\chi$ 时，$\sigma_n(\chi)=0$. 为此，设 $A\in R_1$，$\deg A\geqslant d_\chi$，则 A 可唯一地表示成

$$A=BF_\chi+C,$$

其中

$$B\in R_1,\ \deg B=\deg A-d_\chi\geqslant 0,\ C\in R,\ \deg C\leqslant d_\chi-1.$$

于是

$$\sigma_n(\chi)=\sum_{\substack{A\in R_1\\ \deg A=n}}\chi^*(A)=\sum_{\substack{B\in R_1\\ \deg B=n-d_\chi}}\sum_{\substack{C\in R\\ \deg C\leqslant d_\chi-1}}\chi^*(BF_\chi+C)$$

$$=\sum_B\sum_{\substack{C\in R\\ \deg C\leqslant d_\chi-1}}\chi^*(C)=0.$$

后者是由于 $\chi\neq\chi_0$，并且 C 恰好过 $(R/(F_\chi))^*$ 的完全代表系. 由此结果可知当 $\chi_0\neq\chi\in\hat{K}$ 时，$L(U,\chi)$ 是多项式

$$L(U,\chi)=\sum_{n=0}^{d_\chi-1}\sigma_n(\chi)U^n.$$

代入(1.5.6)，可得到多项式 $F_K(U)$ 的明显表达式. 进而我们计算 $h(K)=F_K(1)$ 的值. 当 χ 是非平凡实特征时，

$$L(1,\chi)=\sum_{n=0}^{d_\chi-1}\sigma_n(\chi)=\sum_{\substack{A\in R_1\\ \deg A\leqslant d_\chi-1}}\chi^*(C).$$

由于 $\chi(F_q^*)=1$，可知

$$L(1,\chi)=\frac{1}{q-1}\sum_{\substack{A\in R\\ \deg A\leqslant d_\chi-1}}\chi^*(C)=0.$$

这表明 $L(U,\chi)/(1-U)$ 是关于 U 的多项式. 并且由洛必达法则可知

$$\left.\frac{L(U,\chi)}{1-U}\right|_{U=1}=\left.\frac{\sum\limits_{n=0}^{d_\chi-1}\sigma_n(\chi)U^n}{1-U}\right|_{U=1}=-\sum_{n=1}^{d_\chi-1}n\sigma_n(\chi)=h(\chi).$$

而当 χ 是 K 的非实特征时，

$$L(1,\chi)=\sum_{n=0}^{d_\chi-1}\sigma_n(\chi)=h(\chi).$$

由于 K 的非平凡实特征共有 $g-1$ 个，从而由(1.5.6)式可知

$$F_K(U)=\prod_{\chi_0\neq\chi\in\hat{K}^+}\left(\frac{L(U,\chi)}{1-U}\right)\cdot\prod_{\chi\in\hat{K}^-}L(U,\chi).$$

这就表明

$$h(K)=F_K(1)=\prod_{\chi_0\neq\chi\in\hat{K}}h(\chi),$$

$$h(K^+)=\prod_{\chi_0\neq\chi\in\hat{K}^+}h(\chi).$$

这就证明了定理1.5.2. ▍

注记　$h(K)/h(K^+)=\prod_{\chi\in\hat{K}^-}h(\chi)$ 称作阿贝尔函数域 K 的相对除子类数，表示成 $h(K)^-$.

系1.5.3　若 $K=k(\Lambda_M)$，$r=\dfrac{\Phi(M)}{q-1}-1$，则

$$\frac{h(O_K)}{h(O_K^+)}=\begin{cases}h(K)^-(q-1)^{-r}, & 若\ M=P^n;\\ h(K)^-(q-1)^{1-r}, & 否则.\end{cases}$$

证明　由于

$$h(K)^-=\frac{h(K)}{h(K^+)}=\frac{h(O_K)}{h(O_K^+)}\cdot\frac{R(O_K)}{R(O_K^+)},$$

再由引理1.3.2即得结果. ▍

例1.5.4　(1) $p=q=2$，$P=P(T)=T^3+T+1$ 是 $R=\mathbf{F}_2[T]$ 中不可约多项式. $K=k(\Lambda_P)$，$k=\mathbf{F}_2(T)$. 由于 $[K:K^+]=q-1=1$，可知 $K=K^+$，$h(K)=h(K^+)$，$h(K)^-=1$. 我们把 T 在 $R/(P)$ 中的像仍记成 T，则 $(R/(P))^*$ 为 $2^3-1=7$ 阶循环群，元素为(注意 $T^3=T+1$)：

$\alpha=T$，$\alpha^2=T^2$，$\alpha^3=1+T$，$\alpha^4=T+T^2$，$\alpha^5=1+T+T^2$，$\alpha^6=1+T^2$.

于是

$$h(K)=\prod_{\substack{\zeta\neq1\\ \zeta^7=1}}[\zeta+\zeta^3+2(\zeta^2+\zeta^4+\zeta^5+\zeta^6)]$$

$$= \prod_{\substack{\zeta\neq 1\\ \zeta^7=1}} (2+\zeta+\zeta^3) = 71.$$

(2) $p=q=5$, $P=T^2+2$是 $R=\boldsymbol{F}_5[T]$中不可约多项式，$k=\boldsymbol{F}_5(T)$，$K=k(\Lambda_P)$. 则 $\alpha=1+T$ 是$24=5^2-1$阶乘法循环群$(R/(P))^*$的生成元. 其中首1多项式用α表示成

$$\alpha^0=1,\ \alpha=1+T,\ \alpha^3=T,\ \alpha^4=3+T,\ \alpha^8=2+T,$$
$$\alpha^{17}=4+T.$$

由于K的实特征群是$24/(5-1)=6$阶循环群，可知

$$h(K^+) = -\prod_{\substack{\zeta\neq 1\\ \zeta^6=1}} (\zeta+\zeta^3+\zeta^4+\zeta^8+\zeta^{17})$$
$$= -\prod_{\substack{\zeta\neq 1\\ \zeta^6=1}} (\zeta+\zeta^3+\zeta^4+\zeta^2+\zeta^5) = -(-1)^5 = 1.$$

另一方面，可以算出

$$h(K)^- = \prod_{\substack{\zeta^6\neq 1\\ \zeta^{24}=1}} (1+\zeta+\zeta^3+\zeta^4+\zeta^8+\zeta^{17}) = 2^{10}\cdot 5^3.$$

由系1.5.3可知

$$h(O_K^+) = 1,\quad h(O_K) = h(O_K^+)\cdot h(K)^-/4^5 = 5^3.$$

第 2 章

分 圆 单 位

一般来说，寻求分圆函数域 $K=k(\Lambda_M)$ 或 K^+ 的一组基本单位系是很困难的. 但是我们可以明显地构作这些域中的一些单位. 取 λ 为一个本原 M-torsion 元素，对每个 $A\in(R/(M))^*$，有

$$\lambda^A/\lambda=\sum_{i=0}^{\deg A}\begin{bmatrix}A\\ i\end{bmatrix}\lambda^{q^i-1}\in R[\lambda],$$

又取 $B\in(R/(M))^*$ 使得 $AB\equiv 1 \pmod M$，则

$$\lambda/\lambda^A=\lambda^{AB}/\lambda^A=\sum_{i=0}^{\deg B}\begin{bmatrix}B\\ i\end{bmatrix}(\lambda^A)^{q^i-1}\in R[\lambda^A]=R[\lambda].$$

这表明 λ^A/λ 是 K 中的单位. 对于每个 $a\in\boldsymbol{F}_q^*$，有

$$\sigma_a(\lambda^A/\lambda)=\sigma_a(\lambda^A)/\sigma_a(\lambda)=\frac{a\lambda^A}{a\lambda}=\frac{\lambda^A}{\lambda}.$$

所以 λ^A/λ 事实上为 K^+ 中的单位. 当 $A=a\in\boldsymbol{F}_q^*$ 时，

$$\lambda^A/\lambda=\frac{a\lambda}{\lambda}=a\in\boldsymbol{F}_q^*.$$

所以我们考虑由集合

$$S=\left\{\frac{\lambda^A}{\lambda}:1\neq A\in R_1,\deg A<\deg M\right\}$$

生成的 U_K^+ 的子群 $C_y(K^+)$，称作**分圆单位群**. 其中每个单位称为**分圆单位**. 有限生成阿贝尔群 $C_y(K^+)$ 的秩就是集合 S 中独立单位的最大个数. 由于 $|S|=|R_1|-1=\dfrac{\Phi(M)}{q-1}-1$，它等于 U_K^+ 的秩. 所以集合 S 是独立的当且仅当 $[U_K^+:\boldsymbol{F}_q^*C_y(K^+)]$ 是有限的. 当 S

是独立的时候,称 S 形成**最大独立单位系**.我们将在§2.1中给出 S 是最大独立单位系的一些判别法.当 S 是最大独立单位系时,我们可算出 $[U_K^+ : F_q^* C_y(K^+)]$ 的值.

§2.1 中的结果表明:在多数情形下,S 不是域 K^+ 的最大独立单位系.我们在§2.2中用 K^+ 和它的子域的分圆单位构作出单位系,它对于任意 M 都是最大独立单位系,并且计算出它在 U_K^+ 中的指数.在§2.3和§2.4中讲述 Sinnott 分圆单位群.对于上述各种分圆单位群,它们在 U_K^+ 中的指数都是理想类数 $h(O_K^+)$ 的整倍数,这就给出 $h(O_K^+)$ 的一种代数解释.在§2.5中我们给出 $h(O_K)/h(O_K^+)$ 的一种代数解释.

§2.1 Kummer-Hilbert 分圆单位系 $C_y(K^+)$

在本节中,我们对任意阿贝尔函数域 K 研究分圆单位系 $C_y(K^+)$ 的秩.设

$k = F_q(T), k \subseteq K \subseteq k(\Lambda_M), M = \mathrm{Cond}(K), d = \deg M \geqslant 1.$

令 $H = \mathrm{Gal}(k(\Lambda_M)/K)$ 为 $\mathrm{Gal}(k(\Lambda_M)/k) = (R/(M))^*$ 的子群,则

$\mathrm{Gal}(K/k) \cong (R/(M))^*/H, \mathrm{Gal}(K^+/k) \cong (R/(M))^*/HF_q^*.$

而 U_K 和 U_K^+ 的秩均为

$$r = [K^+ : k] - 1 = |(R/(M))^*/HF_q^*| - 1.$$

对每个 $A \in (R/(M))^*$,$N_{k(\Lambda_M)^+/K^+}(\lambda^A/\lambda)$ 是 K^+ 中的(分圆)单位.我们取 R 中首1多项式 $A_1, A_2, \cdots, A_r$ ($\deg A_i < d$),使得 $A_0 = 1$,$A_1, \cdots, A_r$ 是 $(R/(M))^*/HF_q^*$ 的完全代表系.令

$$\varepsilon_i = N_{k(\Lambda_M)^+/K^+}(\lambda^{A_i}/\lambda) \quad (1 \leqslant i \leqslant r),$$

以 $C_y(K^+)$ 表示由 $\varepsilon_1, \cdots, \varepsilon_r$ 生成的 U_K^+ 的子群,易知这个群 $C_y(K^+)$ 与完全代表系 $\{A_i\}$ 以及本原 M-torsion 元素 λ 的选取方式无关.如果 $C_y(K^+)$ 的秩为 r,则 $\varepsilon_1, \cdots, \varepsilon_r$ 即是 K 和 K^+ 的最大独立单位系.

定理 2.1.1 在上述记号下,又令

$$g(K^+) = \prod_{\chi_0 \neq \chi \in \hat{K}^+} \prod_{P|M} (1 - \chi^*(P)),$$

则

(1) $\epsilon_1, \cdots, \epsilon_r$ 是 K^+ 的最大独立单位系的充分必要条件为 $g(K^+) = 0$.

(2) 若 $g(K^+) \neq 0$,则

$$[U_K^+ : F_q^* C_v(K^+)] = g(K^+) h(O_K^+).$$

证明 固定∞在 $k(\Lambda_M)$中的一个扩充素除子 $\mathscr{P}$. 则 $k(\Lambda_M)$中全部无限素除子为

$$\mathscr{P}_A = \sigma_A^{-1}(\mathscr{P}) \quad (A \in R_1, (A, M) = 1, \deg A < d).$$

这里 R_1 表示 $R = F_q[T]$中首 1 多项式全体. 以 $\mathscr{P}_A^+$ 表示 $\mathscr{P}_A$ 在 $k(\Lambda_M)^+$中的限制,则 $\mathscr{P}_A^+ = \mathscr{P}_A^{q-1}$. 进而,$\widetilde{\mathscr{P}}_A^+ = N_{k(\Lambda_M)^+/K^+}(\mathscr{P}_A^+)$是 K^+中的无限素除子,并且 $\widetilde{\mathscr{P}}_A^+ = \widetilde{\mathscr{P}}_{A'}^+$当且仅当

$$A \equiv A' (\bmod HF_q^*).$$

所以 $\widetilde{\mathscr{P}}_{A_i}^+ (0 \leqslant i \leqslant r)$就是 K^+的全部无限素除子.

根据定理 1.2.2 和引理 1.2.3,存在本原 M-torsion 元素 λ,使得 $v_{\mathscr{P}}(\lambda) = (q-1)(d-1)-1$,并且对于 $A \in R_1$, $\deg A < d$, 均有

$$v_{\mathscr{P}_A}(\lambda) = v_{\mathscr{P}}(\lambda^A) = (q-1)(d - \deg A - 1) - 1. \tag{2.1.1}$$

令

$$m(A) = v_{\mathscr{P}_A}(\lambda) = v_{\mathscr{P}}(\lambda^A),$$

则当 $\chi_0 \neq \chi \in \hat{K}^+$时,由(2.1.1)式可知

$$\sum_{\substack{A \in R_1 \\ \deg A < d}} \chi(A) m(A) = -(q-1) \sum_{\substack{A \in R_1 \\ \deg A < d}} \chi(A) \deg A, \tag{2.1.2}$$

对每个 $B \in R, (B, M) = 1$,则 $v_{\mathscr{P}_A}(\lambda^B/\lambda) = m(AB) - m(A)$. 由于 λ^B/λ 是 $k(\Lambda_M)^+$中的单位,所以

$$\operatorname{div}(\lambda^B/\lambda) = \prod_{\substack{A \in R_1 \\ \deg A < d}} \mathscr{P}_A^{m(AB)-m(A)} = \prod_{\substack{A \in R_1 \\ \deg A < d}} \mathscr{P}_A^{+(m(AB)-m(A))/(q-1)}.$$

于是

$$\operatorname{div}(\epsilon_i) = \operatorname{div}\left(N_{k(\Lambda_M)^+/K^+}\left(\lambda^{A_i^{-1}}/\lambda \right) \right)$$

$$= \prod_{\substack{A\in R_1 \\ \deg A<d}} \widetilde{\mathscr{D}}_A^{+\,(m(AA_i^{-1})-m(A))/(q-1)}$$

$$= \prod_{\substack{A\in R_1 \\ \deg A<d}} \left(\frac{\widetilde{\mathscr{D}}_A^{+}}{\widetilde{\mathscr{D}}_1^{+}}\right)^{(m(AA_i^{-1})-m(A))/(q-1)}$$

$$= \prod_{j=1}^{r} \left(\frac{\widetilde{\mathscr{D}}_{A_j}^{+}}{\widetilde{\mathscr{D}}_1^{+}}\right)^{m_{ij}},$$

其中

$$m_{ij} = \frac{1}{q-1} \sum_{\substack{A\in R_1 \\ \deg A<d \\ A\equiv A_j (\mathrm{mod}\ HF_q^*)}} (m(AA_i^{-1}) - m(A)) \quad (1\leqslant i,j\leqslant r).$$

由于 $\widetilde{\mathscr{D}}_{A_j}^{+}/\widetilde{\mathscr{D}}_1^{+}$ $(1\leqslant j\leqslant r)$是 $D_{\infty}^0(K^+)$的一组基，所以上式表明 $\mathrm{div}(\varepsilon_j)$ $(1\leqslant j\leqslant r)$对于这组基的变换方阵为$(m_{ij})$. 为了计算这个方阵的特征值，需要如下引理：

引理 2.1.2 设 G 是有限阿贝尔群，f 是由 G 到复数域 $\boldsymbol{C}$ 上的函数，则方阵$(f(\sigma\tau^{-1}))_{\sigma,\tau\in G}$的特征值为$\sum_{\sigma\in G}\chi(\sigma)f(\sigma)$ $(\chi\in\hat{G})$. 而方阵

$$(f(\sigma\tau^{-1}) - f(\sigma))_{\sigma,\tau\neq 1}$$

的特征值为$\sum_{\sigma\in G}\chi(\sigma)f(\sigma)$ $(\chi\in\hat{G},\chi\neq\chi_0)$.

证明 见文献[57]中第 71～72 页，引理 5.2.6. ∎

在引理 2.1.2 中取 $G=\mathrm{Gal}(K^+/k)$，而 $A_0=1,A_1,\cdots,A_r$ 是群 G 的代表元素. 函数 $f:G\to\boldsymbol{C}$ 取为

$$f(A_i) = \frac{1}{q-1} \sum_{\substack{A\in R_1 \\ \deg A<d \\ A\equiv A_i (\mathrm{mod}\ HF_q^*)}} m(A).$$

由引理 2.1.2 即知方阵$(m_{ij})_{1\leqslant i,j\leqslant r}$的 r 个特征值为

$$\frac{1}{q-1}\sum_{i=0}^{r} \sum_{\substack{A\in R_1 \\ \deg A<d \\ A\equiv A_i (HF_q^*)}} \chi(A)m(A) = \frac{1}{q-1} \sum_{\substack{A\in R_1 \\ \deg A<d}} \chi(A)m(A)$$

$$= -\sum_{\substack{A\in R_1\\ \deg A<d}}\chi(A)\deg A$$

(由(2.1.2)式)

$$(\chi_0\neq\chi\in\hat{K}^+).$$

引理 2.1.3 设 $\chi_0\neq\chi\in\hat{K}^+$, $d_\chi=\deg(F_\chi)$, 则

$$\sum_{\substack{A\in R_1\\ \deg A<d}}\chi(A)\deg A=\Big(\sum_{\substack{A\in R_1\\ \deg A<d_\chi}}\chi^*(A)\deg A\Big)\prod_{P\mid M}(1-\chi^*(P)).$$

证明 以 $P_1,\cdots,P_t$ 表示满足 $P\mid M$, $P\nmid F_\chi$ 的所有首1不可约多项式 P, $d_i=\deg P_i$. 则

$$\begin{aligned}\sum_{\substack{A\in R_1\\ \deg A<d}}\chi(A)\deg A=&\sum_{\substack{A\in R_1\\ \deg A<d\\ (A,M)=1}}\chi^*(A)\deg A\\ =&\sum_{\substack{A\in R_1\\ \deg A<d}}\chi^*(A)\deg A\\ &-\sum_{i=1}^{t}\chi^*(P_i)\sum_{\substack{A\in R_1\\ \deg A<d-d_i}}\chi^*(A)\deg(P_iA)\\ &+\sum_{1\leqslant i<j\leqslant t}\chi^*(P_iP_j)\sum_{\substack{A\in R_1\\ \deg A<d-d_i-d_j}}\chi^*(A)\deg(P_iP_jA)\\ &-\cdots+(-1)^t\chi^*(P_1\cdots P_t)\\ &\times\sum_{\substack{A\in R_1\\ \deg A<d-d_1-\cdots-d_t}}\chi^*(A)\deg(P_1\cdots P_tA).\end{aligned}\tag{2.1.3}$$

由 $P_i\nmid F_\chi$ $(1\leqslant i\leqslant t)$ 可知 $F_\chi\Big|\dfrac{M}{P_1\cdots P_t}$. 特别地, $d_\chi\leqslant d-d_1\cdots-d_t$. 因此

$$\sum_{\substack{A\in R_1\\ \deg A<d-d_i}}\chi^*(A)\deg(AP_i)=\sum_{\substack{A\in R_1\\ \deg A<d-d_i}}\chi^*(A)\deg A,$$

$$\cdots\cdots\cdots\cdots$$

$$\sum_{\substack{A\in R_1\\ \deg A<d-d_1-\cdots-d_t}}\chi^*(A)\deg(AP_1\cdots P_t)=\sum_{\substack{A\in R_1\\ \deg A<d-d_1-\cdots-d_t}}\chi^*(A)\deg A.$$

现在对每个 $d'\geqslant d_\chi$，有

$$\sum_{\substack{A\in R_1\\ \deg A<d'}}\chi^*(A)\deg A=(q-1)^{-1}\sum_{\substack{A\in R\\ \deg A<d'}}\chi^*(A)\deg A$$

$$=(q-1)^{-1}\sum_{\substack{C\in R\\ \deg C<d_\chi}}\sum_{\substack{B\in R\\ \deg B<d'-d_\chi}}\chi^*(BF_\chi+C)$$

$$\times\deg(BF_\chi+C)$$

$$=(q-1)^{-1}\sum_C\sum_B\chi^*(C)\deg(BF_\chi+C)$$

$$=(q-1)^{-1}\sum_C\chi^*(C)\deg C$$

$$=\sum_{\substack{A\in R_1\\ \deg A<d_\chi}}\chi^*(A)\deg A,$$

代入(2.1.3)式即得

$$\sum_{\substack{A\in R_1\\ \deg A<d}}\chi(A)\deg A=\Big(\sum_{\substack{A\in R_1\\ \deg A<d_\chi}}\chi^*(A)\deg A\Big)\Big(1-\sum_{i=1}^{t}\chi^*(P_i)$$

$$+\sum_{1\leqslant i<j\leqslant t}\chi^*(P_iP_j)-\cdots+(-1)^t\chi^*(P_1\cdots P_t)\Big)$$

$$=\Big(\sum_{\substack{A\in R_1\\ \deg A<d_\chi}}\chi^*(A)\deg A\Big)\prod_{P|M}(1-\chi^*(P)).$$

这就证明了引理 2.1.3. ▌

往下继续证明定理 2.1.1. 对每个 $\chi_0\neq\chi\in\hat{K}^+$，记 $h(\chi)=-\sum_{\substack{A\in R_1\\ \deg A<d_\chi}}\chi^*(A)\deg A$. 由于 $h(K^+)=\prod_{\chi_0\neq\chi\in\hat{K}^+}h(\chi)$(定理 1.5.2)，可知 $h(\chi)\neq0$. 但是方阵(m_{ij})的特征值为

$$h(\chi)\prod_{P|M}(1-\chi^*(P))\quad(\chi_0\neq\chi\in\hat{K}^+),$$

所以 $\mathrm{div}(\epsilon_i)$ $(1\leqslant i\leqslant r)$当中独立的最大个数(即方阵$(m_{ij})$的秩)等于满足$\prod_{P|M}(1-\chi^*(P))$的 $\hat{K}^+$ 中非平凡实特征的个数，并且这也等于分圆单位群 $C_y(K^+)$的秩. 特别地，$C_y(K^+)$的秩为 r 当且仅

当 $g(K^+)\neq 0$. 并且当 $g(K^+)\neq 0$ 时,

$$
\begin{aligned}
[D^0_{\infty}(K^+):\mathrm{div}(C_y(K^+))] &= |\deg(m_{ij})| \\
&= \prod_{\chi_0\neq\chi\in\hat{K}^+}\left(h(\chi)\prod_{P|M}(1-\chi^*(P))\right) \\
&= h(K^+)g(K^+).
\end{aligned}
$$

但是

$$[D^0_{\infty}(K^+):\mathrm{div}(U_K^+)] = R(O_K^+) = h(K^+)/h(O_K^+),$$

于是

$$
\begin{aligned}
[U_K^+:\mathbb{F}_q^* C_y(K^+)] &= [\mathrm{div}(U_K^+):\mathrm{div}(C_y(K^+))] \\
&= g(K^+)h(O_K^+).
\end{aligned}
$$

这就完成了定理 2.1.1 的证明. ▮

注记 当 $\mathrm{Cond}(K^+)=P^n$ 时,对每个 $\chi_0\neq\chi\in\hat{K}^+$, $F_\chi=P^m$, $m\geqslant 1$,因此 $\chi^*(P)=0$,即 $g(K^+)=1$. 从而 $[U_K^+:\mathbb{F}_q^* C_y(K^+)]=h(O_K^+)$. 这种情形在文献[35]中有证明. 而对定理 2.1.1 的一般情形在文献[7]中有证明.

下面给出 $g(K^+)$ 的一个数论解释. 特别是可知 $g(K^+)$ 是非负整数. 记

$$g(P) = \prod_{\chi_0\neq\chi\in\hat{K}^+}(1-\chi^*(P)),$$

则 $g(K^+)=\prod_{P|M} g(P)$. 若 P 在 K^+ 中的惰性域和分解域分别是 K_I 和 K_D,则定理 1.4.1 表明了:

$$\hat{K}_I = \{\chi\in\hat{K}^+:\chi^*(P)\neq 0\},\ \hat{K}_D = \{\chi\in\hat{K}^+:\chi^*(P)=1\}.$$

令 f_P 和 g_P 分别表示 P 对于 $\hat{K}^+$ 的剩余类域次数和分解次数,则

$$[\hat{K}_I:\hat{K}_D] = [K_I:K_D] = f_P,\quad [K_D:k] = g_P = |\hat{K}_D|.$$

于是

$$g(P) = \prod_{\chi_0\neq\chi\in\hat{K}_I}(1-\chi^*(P)),$$

并且

$$g(P) = 0 \Longleftrightarrow |\hat{K}_D| \geqslant 2 \Longleftrightarrow g_P \geqslant 2.$$

当 $g_P=1$ 时，$\hat{K}_D=k$，而 $\hat{K}_I$ 中所有特征相结合的本原特征在 P 的取值恰是 f_P 个不同的 f_P 次单位根. 于是

$$g(P)=\prod_{\chi_0\neq\chi\in\hat{K}_I}(1-\chi^*(P))=\prod_{\substack{\zeta^{f_P}=1\\ \zeta\neq1}}(1-\zeta)=f_P\quad(\text{当 } g_P=1$$

时). 这就表明

$$g(K^+)\neq0\Longleftrightarrow \text{对每个 } P|M,\ g_P=1$$
$$\Longrightarrow g(K^+)=\prod_{P|M}f_P.$$

进而，若 $M=P^nN$，$(N,P)=1$，则 $K_I=K^+\cap k(\Lambda_N)$. 由于 $\mathrm{Gal}(K^+/k)$ 被看成为 $(R/(M))^*/HF_q^*$，所以 $\mathrm{Gal}(K_I/k)$ 被看成为 $(R/(N))^*/F_q^*H_P$，其中 H_P 是 H 在自然投射

$$(R/(M))^*\to(R/(N))^*$$

之下的象. 由于 $\mathrm{Gal}(K_I/K_D)$ 是 $(R/(N))^*/F_q^*H_P$ 中由 P 生成的 f_P 阶循环群，所以

$$g_P=1\Longleftrightarrow K_D=k\Longleftrightarrow\hat{K}_D=\{\chi_0\}$$

$\Longleftrightarrow$ 对 $(R/(N))^*/F_q^*H_P$ 中每个特征 χ，若 $\chi^*(P)=1$，则 $\chi=\chi_0\Longleftrightarrow(R/(N))^*/\langle F_q^*H_P,P\rangle$ 只有平凡特征

$$\Longleftrightarrow(R/(N))^*=\langle F_q^*H_P,P\rangle,$$

其中 $\langle F_q^*H_P,P\rangle$ 表示由 $F_q^*H_P$ 和 P 生成的 $(R/(N))^*$ 的子群. 综合上述，我们得到 K^+ 的分圆单位系 $\varepsilon_1,\cdots,\varepsilon_r$ 独立的如下一些判别法.

定理 2.1.4 设 $k=F_q(T)$，$k\subsetneq K\subsetneq k(\Lambda_M)$，$M=\mathrm{Cond}(K)$，$M=\prod_{i=1}^{t}P_i^{r_i}$，其中 $P_1,\cdots,P_t$ 是 M 的不同首 1 不可约因子. 以 f_i 和 g_i 分别表示 P_i 在 K^+ 中的剩余类域次数和分解次数. 又令 $H=\mathrm{Gal}(k(\Lambda_M)/K)$（可看成为 $\mathrm{Gal}(k(\Lambda_M)/k)=(R/(M))^*$ 的子群）. 以 H_i 表示 H 在自然投射

$$(R/(M))^*\to(R/(M_i))^*\quad(M_i=M/P_i^{r_i})$$

之下的象.

$$r=|(R/(M))^*/F_q^*H|-1=[K^+:k]-1.$$

则下列三个条件彼此等价：

(1) $\varepsilon_i(1\leqslant i\leqslant r)$是 K^+(和 K)中最大独立单位系.

(2) $g_i=1 \quad (1\leqslant i\leqslant t)$.

(3) 对每个 $i(1\leqslant i\leqslant t)$，$(R/(M_i))^*=\langle \boldsymbol{F}_q^* H_i, P_i\rangle$.

当且仅当这些条件成立时，$g(K^+)=\prod\limits_{i=1}^{t} f_i$ (否则，$g(K^+)=0$). 其中 f_i 也等于 P_i 在 $(R/(M_i))^*/\boldsymbol{F}_q^* H_i$ 中的阶. ▌

作为定理 2.1.4 的一个应用，则有：

系 2.1.5　令 $K=k(\Lambda_M)$，则当 $q\geqslant 3$ 并且 M 至少有 4 个不同的首 1 不可约因子时，K^+的分圆单位系

$$\{\lambda^A/\lambda : 1\neq A\in R_1, \deg A<\deg M\}$$

不是独立的.

证明　这时 $H=1$，$M=\prod\limits_{i=1}^{t} P_i^{e_i}$，$t\geqslant 4$. 对于 $M_1=M/P_1^{e_1}$，我们有

$$(R/(M_1))^* = \prod_{i=2}^{t}(R/(P_i^{e_i}))^* \quad (\text{直积}).$$

令 l 为 $q-1(\geqslant 2)$的一个素因子. 由于每个$(R/(P_i^{e_i}))^*$都有 l 阶子群，所以有限阿贝尔群 $(R/(M_1))^*$ 的 l-秩 $\geqslant t-1\geqslant 3$. 于是 $(R/(M_1))^*/\boldsymbol{F}_q^*$ 的 l-秩$\geqslant 2$，所以不能是由 P_1 生成的循环群. 因此 $(R/(M_1))^*\neq\langle \boldsymbol{F}_q^*, P_1\rangle$. 由定理 2.1.4 即知定理中的分圆单位系不是独立的. ▌

注记　在文献[7]中决定出系 2.1.5 中分圆单位系独立的全部分圆函数域 $k(\Lambda_M)$.

§ 2.2　Levesque 和 Ramachandra 分圆单位系

本节利用子域中的分圆单位，对每个阿贝尔函数域 K 均构作一组最大独立的分圆单位系. 我们保持上节中的符号：

$$k=\boldsymbol{F}_q(T),\ k\subseteq K\subseteq k(\Lambda_M),\ M=\mathrm{Cond}(K),$$

$$\mathrm{Gal}(k(\Lambda_M)/K) = H \subseteq (R/(M))^*,$$

$$\mathrm{Gal}(K^+/k) \cong (R/(M))^*/HF_q^*,\quad r = [K^+:k] - 1.$$

取 $A_1,\cdots,A_r \in R_1$，$\deg A_i < d = \deg M$，使得 $A_0 = 1, A_1,\cdots,A_r$ 是 $(R/(M))^*/HF_q^*$ 的完全代表系.

设 λ 是一个本原 M-torsion 元素，则对 M 的每个首 1 多项式因子 $D(\deg D < \deg M)$，λ^D 是本原$\frac{M}{D}$-torsion 元素，而 $\lambda^{DA_i^{-1}}/\lambda^D$ 是 $k(\Lambda_{M/D})^+$ 中的(分圆)单位. 从而 $N_{k(\Lambda_M)^+/K^+}(\lambda^{DA_i^{-1}}/\lambda^D)$ 也是 K^+ 中的单位. 更一般地，令

$$\mathscr{S}_M = \{D \in R_1 : D|M, D \neq M\},$$

而 $\mathscr{D}$ 为 $\mathscr{S}_M$ 中任一非空子集合，则

$$\varepsilon_i = \varepsilon_i(\mathscr{D}) = N_{k(\Lambda_M)^+/K^+}\Big(\prod_{D\in\mathscr{D}} \lambda^{DA_i^{-1}}/\lambda^D\Big) \quad (1 \leqslant i \leqslant r) \tag{2.2.1}$$

均是 K^+ 中单位. 我们把 $\varepsilon_1,\cdots,\varepsilon_r$ 称作 K^+关于 $\mathscr{D}$ 的 Levesque 分圆单位系，因为它是文献[45]中 Levesque 对于数域情形的单位系在函数域的模拟. 以 $C_y(\mathscr{D},K^+)$表示由 $\varepsilon_i(\mathscr{D})$ $(1\leqslant i\leqslant r)$生成的 U_K^+ 的子群. 这个群和本原 M-torsion 元素 λ 的选取方式无关. 当 $\mathscr{D}=\{1\}$时，它就是上节的单位群 $C_y(K^+)$. 现在我们决定何时 $\varepsilon_i(\mathscr{D})$ $(1\leqslant i\leqslant r)$为最大独立单位系. 并且当它们独立时，我们计算$[U_K^+ : F_q^* C_y(\mathscr{D},K^+)]$的值.

定理 2.2.1 在上述记号下，又令

$$i(\mathscr{D}) = \prod_{\chi_0\neq\chi\in\hat{K}^+}\left[\sum_{\substack{D\in\mathscr{D}\\ F_\chi | \frac{M}{D}}}\frac{\Phi(M)}{\Phi\left(\frac{M}{D}\right)}\prod_{P|\frac{M}{D}}(1-\chi^*(P))\right],$$

则

(1) 单位系 $\varepsilon_i(\mathscr{D})$ $(1\leqslant i\leqslant r)$独立的充分必要条件为 $i(\mathscr{D})\neq 0$.

(2) 当 $i(\mathscr{D})\neq 0$ 时，$[U_K^+ : F_q^* C_y(\mathscr{D},K^+)] = i(\mathscr{D})h(O_K^+)$.

证明 取 $\mathscr{P}$ 为 $k(\Lambda_M)$中一个无限素除子. 则存在本原 M-torsion 元素 λ，使得 $v_{\mathscr{P}}(\lambda) = (q-1)(\deg M - 1) - 1$. 并且对每个 $A \in$

R，$\deg A<\deg M$，均有 $v_{\mathscr{P}}(\lambda^A)=(q-1)(\deg M-\deg A-1)-1$. 对 $R/(M)$ 中每个元素 A，记 $m(A)=v_{\mathscr{P}}(\lambda^A)$. 以 $\widetilde{\mathscr{P}}^+$ 表示 $\mathscr{P}$ 在 K^+ 中的限制，而令

$$\widetilde{\mathscr{P}}^+_{A_j}=\sigma(A_j)^{-1}(\widetilde{\mathscr{P}}^+)\quad(1\leqslant j\leqslant r),$$

则对于由(2.2.1)式定义的 $\varepsilon_i=\varepsilon_i(\mathscr{D})\in U_K^+$，与证明定理 2.1.1 一样地得到

$$\operatorname{div}(\varepsilon_i)=\prod_{j=1}^{r}\left(\widetilde{\mathscr{P}}^+_{A_j}/\widetilde{\mathscr{P}}^+_1\right)^{m_{ij}}\quad(1\leqslant i\leqslant r),$$

其中(记 $d=\deg M$)

$$m_{ij}=(q-1)^{-1}\sum_{\substack{A\in R_1\\ \deg A<d\\ A\equiv A_j(\mathrm{mod}\,\mathbb{F}_q^*)}}\sum_{D\in\mathscr{D}}(m(AA_i^{-1}D)-m(AD)).$$

我们只需再证明

$$\left|\det(m_{ij})_{1\leqslant i,j\leqslant r}\right|=h(K^+)i(\mathscr{D}),\qquad(2.2.2)$$

然后即得定理 2.2.1. 为证(2.2.2)式，我们在引理 2.1.2 中取 $G=\mathrm{Gal}(K^+/k)$，($A_0=1,A_1,\cdots,A_r$ 是此群的完全代表系)，取函数 $f:G\to\mathbf{C}$ 为

$$f(A_i)=(q-1)^{-1}\sum_{\substack{A\in R_1\\ \deg A<d\\ A\equiv A_i(\mathrm{mod}\,\mathbb{F}_q^*)}}\sum_{D\in\mathscr{D}}m(AD),$$

便得到

$$\begin{aligned}\det(m_{ij})&=(q-1)^{-r}\prod_{\chi_0\neq\chi\in\hat{K}^+}\sum_{i=0}^{r}\sum_{\substack{A\in R_1\\ \deg A<d\\ A\equiv A_i(\mathrm{mod}\,\mathbb{F}_q^*)}}\chi(A)\sum_{D\in\mathscr{D}}m(AD)\\&=(q-1)^{-r}\prod_{\chi_0\neq\chi\in\hat{K}^+}\sum_{\substack{A\in R_1\\ \deg A<d}}\chi(A)\sum_{D\in\mathscr{D}}m(AD)\\&=(q-1)^{-2r}\prod_{\chi_0\neq\chi\in\hat{K}^+}\sum_{A\in(R/(M))^*}\chi(A)\sum_{D\in\mathscr{D}}m(AD).\end{aligned}$$

(2.2.3)

现在我们证明以下引理：

引理 2.2.2 设 $D\in\mathscr{S}_M$，$N=\dfrac{M}{D}$，χ 为模 M 特征，则

$$\sum_{A\in(R/(M))^*}\chi(A)m(AD)=\begin{cases}\dfrac{\Phi(M)}{\Phi(N)}\cdot\displaystyle\sum_{B\in(R/(N))^*}\chi(B)m(BD), & \text{若 } F_\chi\mid N;\\ 0, & \text{否则}.\end{cases}$$

证明 将上式左端记为 L. 当 $F_\chi\nmid N$ 时，存在 $B\in R$，$(B,M)=1$，$B\equiv 1\pmod N$，使得 $\chi(B)\neq 1$. 由 $BD\equiv D\pmod M$ 可知

$$L=\sum_{A\in(R/(M))^*}\chi(AB)m(ABD)$$

$$=\sum_{A\in(R/(M))^*}\chi(A)\chi(B)m(AD)=\chi(B)L,$$

所以 $L=0$. 当 $F_\chi\mid N$ 时，

$$L=\sum_{\substack{\deg B<\deg N\\(B,N)=1}}\ \sum_{\substack{\deg C<\deg D\\(B+CN,M)=1}}\chi(B+CN)m(D(B+CN))$$

$$=\sum_B\chi(B)m(BD)\sum_C 1=\frac{\Phi(M)}{\Phi(N)}\sum_{B\in(R/(N))^*}\chi(B)m(BD).$$

这就证明了引理 2.2.2.

将引理 2.2.2 的结果代入(2.2.3)式，便得到

$$\det(m_{ij})=(q-1)^{r}\prod_{\chi_0\neq\chi\in\hat{K}^{+}}\ \sum_{\substack{D\in\mathscr{S}_M\\F_\chi\mid\frac{M}{D}}}\frac{\Phi(M)}{\Phi\left(\frac{M}{D}\right)}\sum_{\substack{A\in R_1\\\deg A<d-\deg D}}\chi(A)m(AD).$$

但是当 $F_\chi\left|\dfrac{M}{D}\right.$ 时，

$$\sum_{\substack{A\in R_1\\\deg A<d-\deg D}}\chi(A)m(AD)=\sum_{\substack{A\in R_1\\\deg A<d-\deg D}}\chi(A)[(d-\deg(AD)-1)(q-1)-1]$$

$$=-(q-1)\sum_{\substack{A\in R_1\\\deg A<d-\deg D}}\chi(A)\deg A$$

$$=(q-1)\Big(\prod_{P\mid\frac{M}{D}}(1-\chi^*(P))\Big)h(\chi)$$

(引理 2.1.3).

于是

$$\det(m_{ij})=\prod_{\chi_0\neq\chi\in\hat{K}^+}h(\chi)\left\{\sum_{\substack{D\in\mathscr{D}\\F_\chi\mid\frac{M}{D}}}\frac{\Phi(M)}{\Phi\left(\frac{M}{D}\right)}\prod_{P\mid\frac{M}{D}}(1-\chi^*(P))\right\}$$

$$=h(K^+)i(\mathscr{D}).$$

这就证明了(2.2.2)式,从而也完成了定理 2.2.1 的证明. ∎

现在我们取 $\mathscr{S}_M$ 的一些特殊子集合 $\mathscr{D}$,使得 $i(\mathscr{D})\neq 0$. 设 $M=\prod_{i=1}^{t}P_i^{n_i}$,其中 $P_1,\cdots,P_t$ 是 M 的不同首 1 不可约因子. 令 $L=\{1,2,\cdots,t\}$,定义 L 的子集合:

$$J_0=\{i\in L:\text{存在}\ \chi_0\neq\chi\in\hat{K}^+\ \text{使得}\ \chi(P_i)=1\}.$$

定理 2.2.3 对每个集合 J,$J_0\subseteq J\subseteq L$,令

$$\mathscr{D}=\mathscr{D}(J)=\{M_I=\prod_{i\in I}P_i^{n_i}:I\subseteq J,I\neq L\},$$

则

$$i(\mathscr{D})=\prod_{\chi_0\neq\chi\in\hat{K}^+}\left[\prod_{\substack{i\in J\\P_i\nmid F_\chi}}(\Phi(P_i^{n_i})+1-\chi^*(P_i))\right.$$

$$\left.\times\prod_{j\in L-J}(1-\chi^*(P_j))\right]\neq 0.$$

证明 由定理 2.2.1 可知 $i(\mathscr{D})=\prod_{\chi_0\neq\chi\in\hat{K}^+}i(\chi)$, 其中

$$i(\chi)=\sum_{\substack{I\subseteq J\\F_\chi\mid M_{L-I}}}\left[\Phi(M_I)\prod_{j\in L-I}(1-\chi^*(P_j))\right]$$

$$=\left(\prod_{j\in L-J}(1-\chi^*(P_j))\right)\sum_{\substack{I\subseteq J\\F_\chi\mid M_{L-I}}}\left[\Phi(M_I)\prod_{i\in J-I}(1-\chi^*(P_i))\right].$$

令 $$J'=\{i\in J:\chi^*(P_i)\neq 0\}=\{i\in J:P_i\nmid F_\chi\},$$

则当 $I\subseteq J$ 时,易知 $F_\chi\mid M_{L-I}\Leftrightarrow I\subseteq J'$. 并且当 $I\subseteq J'$ 时,

$$\prod_{j\in J-I}(1-\chi^*(P_j))=\prod_{j\in J'-I}(1-\chi^*(P_j)),$$

于是

$$i(\chi)=\Big(\prod_{j\in L-J}(1-\chi^*(P_j))\Big)\times\sum_{I\subseteq J'}\Big[\Big(\prod_{i\in I}\Phi(P_i^{n_i})\Big)\Big(\prod_{i\in J'-I}(1-\chi^*(P_i))\Big)\Big]$$

$$=\prod_{j\in L-J}(1-\chi^*(P_j))\prod_{i\in J'}(\Phi(P_i^{n_i})+1-\chi^*(P_i))$$

$$=\prod_{j\in L-J}(1-\chi^*(P_j))\prod_{\substack{i\in J\\ P_i\nmid F_\chi}}(\Phi(P_i^{n_i})+1-\chi^*(P_i)).$$

由 $J_0\subseteq J$ 可知 $i(\chi)\neq 0$，从而 $i(\varnothing)\neq 0$. 即证明定理 2.2.3. ∎

特别地，取 $J=L$，我们对 $k(\Lambda_M)$ 的每个实阿贝尔子域 K^+ 均得到一组最大独立分圆单位系 $(\epsilon_1,\cdots,\epsilon_r)$，其中

$$\Big(令\ M=\prod_{i=1}^{t}P_i^{n_i},\ L=\{1,2,\cdots,t\}\Big)$$

$$\epsilon_i=N_{k(\Lambda_M)^+/K^+}\Big(\prod_{\substack{l\in L\\ l\neq L}}\lambda^{M_lA_i^{-1}}/\lambda^{M_l}\Big).$$

这组分圆单位系是数域情形 Ramachandra 单位系（参见文献[57]中的定理 8.3）的模拟. 若以 $C_y(K^+)_R$ 表示这组单位系生成的群，则

$$[U_K^+:F_q^*C_y(K^+)_R]$$

$$=h(O_K^+)\prod_{\chi_0\neq\chi\in\hat{K}^+}\prod_{\substack{i=1\\ P_i\nmid F_\chi}}^{t}(\Phi(P_i^{n_i})+1-\chi^*(P_i)).$$

§2.3 Sinnott 分圆单位群

固定 $F_q[T]$ 中一个首 1 多项式 $M=M(T)$，$d=\deg M\geqslant 1$，$k=F_q(T)$，$K=k(\Lambda_M)$. 对于本原 M-torsion 元素 λ，§2.1 中的结果表明由 $\{\lambda^A/\lambda:(A,M)=1\}$ 生成的分圆单位群的秩可能小于 $r=\dfrac{\Phi(M)}{q-1}-1=[K^+:k]-1$. 现在我们考虑一个更大的群. 令 P 是由 F_q^* 和 $\Lambda_M^*=\Lambda_M-\{0\}$ 生成的 K^* 的乘法子群. 我们把

$$C=P\cup U_K$$

称作 K 的 Sinnott 分圆单位群. 注意, 对每个 $\lambda\in\Lambda_M^*$ 和 $\sigma\in G=\mathrm{Gal}(K/k)$, $\lambda^{\sigma-1}=\lambda^\sigma/\lambda\in C$. 因此 $P^{\sigma-1}\subseteq C$. 此外, 若 M' 是 M 的首 1 多项式因子, λ' 是本原 M'-torsion 元素, 则对于 $\sigma\in G$, $(\lambda')^{\sigma-1}$ 是 K 的子域 $k(\Lambda_{M'})$ 中的分圆单位. 这就表明 C 是由 K 和它的子域的所有分圆单位(以及 F_q^*)生成的群. Sinnott[9] 于 1978 年对于分圆数域 $\boldsymbol{Q}(\zeta_m)$ 研究了类似的群, 证明了对于每个 $m\geqslant2$, 它在整个单位群中的指数均为有限的, 并且计算出了这个指数. 对于分圆函数域的情形, 沿用 Sinnott 的方法, Galovich 和 Rosen[6] 作了类似的计算, 得到了如下的结果:

定理 2.3.1　以 g 表示 M 的不同首 1 不可约因子的个数, $U=U_K$ 为 $K=k(\Lambda_M)$ 的单位群, $k=\boldsymbol{F}_q(T)$, C 是上面定义的Sinnott分圆单位群. 则

$$[U:C]=h(O_K^+)(q-1)^a,$$

其中当 $g=1$ 时 $a=0$, 而当 $g\geqslant2$ 时 $a=2^{g-2}+1-g$.

注记　令 $U^+=U_K^+$, $C^+=C\cap U^+$. 当 $g=1$ 时 $U=U^+$, 而当 $g\geqslant2$时, 我们知道 $\lambda\in U$, 而 $1,\lambda,\lambda^2,\cdots,\lambda^{q-2}$ 是 U 对 U^+ 的陪集代表系, $[U:U^+]=q-1$. 由于 $\lambda\in C$, 从而我们总有 $U=U^+C$. 于是

$$[U:C]=[U^+C:C]=[U^+:C\cap U^+]=[U^+:C^+].$$

对于 $g=1$ 的情形, C^+ 就是 §2.1 中定义的 $\boldsymbol{F}_q^*C_v(K^+)$. 对于这种情形, 定理 2.3.1 已经证明了(即定理 2.1.1).

定理 2.3.1 的证明是通过相当精细的计算. 我们将在下节完成这个计算. 注意, P、C 和 U 均是 $\boldsymbol{Z}[G]$-模. 我们还需要考查它们的一些子模的结构. 对于 $G=\mathrm{Gal}(K/k)$的每个子集 H, 记

$$s(H)=\sum_{\sigma\in H}\sigma\in\boldsymbol{Z}[G].$$

并且令

$$M=\prod_{i=1}^{g}Q_i^{e_i},d_i=\deg Q_i,\quad M_i=\frac{M}{Q_i^{e_i}},$$

其中 $Q_1,\cdots,Q_g$ 是 M 的不同的首 1 不可约因子.

引理 2.3.2　(1) 对于 $a\in P$, 则

$$\alpha \in C \Leftrightarrow \alpha^{s(G)} = 1,\quad \alpha \in \boldsymbol{F}_q^* \Leftrightarrow \alpha^{s(J)} = 1,$$

其中 $J=\{\sigma_a : a\in \boldsymbol{F}_q^*\}$.

(2) $P^{s(G)} = \left\{\prod_{i=1}^{g} Q_i^{\Phi(M_i)k_i} : k_i\in \boldsymbol{Z}\right\}$.

证明　(1) 若 $\alpha\in C=P\cap U$，则 $\alpha^{s(G)}=N_{K/k}(\alpha)\in \boldsymbol{F}_q^*$. 但是对 P 的每个生成元 $\beta\in \boldsymbol{F}_q^*\cup\Lambda_M^*$，$\beta^{s(G)}$ 是 $\boldsymbol{F}_q[T]$ 中的首 1 多项式. 于是 $\alpha^{s(G)}=1$. 反之，若 $\alpha^{s(G)}=1$，显然 $\alpha\in P\cup U=C$.

如果 $\alpha\in \boldsymbol{F}_q^*$，则 $\alpha^{s(J)}=\alpha^{q-1}=1$. 反之，若 $\alpha^{s(J)}=1$. 由于对 P 的每个生成元 β 均有 $\beta^{s(J)}=\pm\beta^{q-1}$. 于是 $\alpha^{q-1}=\pm\alpha^{s(J)}=\pm 1$. 由于乘法群 K^* 的 torsion 子群为 $\boldsymbol{F}_q^*$，于是 $\alpha\in \boldsymbol{F}_q^*$.

(2) 乘法群 P 是由 $\boldsymbol{F}_q^*$ 和 Λ_M^* 生成的. 对于 $c\in \boldsymbol{F}_q^*$，有 $c^{s(G)}=c^{|G|}=1$（因为 $(q-1)\mid\Phi(M)=|G|$）. 对于 $\mu\in\Lambda_M^*$，若 μ 为本原 N-torsion 元素，$N\mid M$，则当 N 不是某个不可约多项式的幂时，μ 为单位，于是 $\mu^{s(G)}=1$. 若 $N=Q^n$（Q 不可约），则

$$\begin{aligned}\mu^{s(G)} &= N_{K/k}(\mu)\\ &= N_{k(\Lambda_{Q^n})/k}(\mu)^a = Q^a,\end{aligned}$$

其中 $a=[K:k(\Lambda_{Q^n})]=\Phi(M)/\Phi(Q^n)$. 即得(2)中的结论. ∎

现在固定 K 的一个无限素除子 $\mathscr{P}$. 对于 $B\in(R/(M))^*$，令 $\mathscr{P}_B=\sigma_B^{-1}(\mathscr{P})$. 考虑映射

$$l: K^*\to \boldsymbol{Q}[G],\quad l(\alpha)=\sum_{B\in(R/(M))^*} v_{\mathscr{P}_B}(\alpha)\sigma_B^{-1}.$$

这是 $\boldsymbol{Z}[G]$-模同态.

引理 2.3.3　(1) $\ker(l)\cap C=\ker(l)\cap U=\boldsymbol{F}_q^*$.

(2) $\ker(l)\cap P=\mathscr{N}$，其中

$$\mathscr{N}=\boldsymbol{F}_q^*\times\left\{\prod_{i=1}^{g} Q_i^{k_i/(q-1)} : k_i\in \boldsymbol{Z},\ \sum_{i=1}^{g} d_ik_i=0\right\}.$$

特别地，阿贝尔群 N 的秩为 $g-1$.

证明　(1) 这是由于对于 $\alpha\in K^*$，$\alpha\in\ker(l)\Leftrightarrow$ 对 K 的每个无限素除子 q，$v_q(\alpha)=0$. 而 $\alpha\in U\Leftrightarrow$ 对 K 的每个有限素除子 q，$v_q(\alpha)=0$. 最后，$\alpha\in \boldsymbol{F}_q^*\Leftrightarrow$ 对 K 的每个素除子 q，$v_q(\alpha)=0$. 由此即

得结论.

(2) 设 λ_i 为本原 Q_i-torsion 元素,则

$$a = \prod_{\substack{A \in (R/(Q_i))^* \\ A \in K_1}} \lambda_i^{\sigma_A} \in P.$$

而

$$Q_i = \prod_{A \in (R/(Q_i))^*} \lambda_i^{\sigma_A} = \prod_{\substack{A \in (R/(Q_i))^* \\ A \in K_1}} \prod_{C \in F_q^*} (C\lambda^{\sigma_A})$$

$$= \Big(\prod_{C \in F_q^*} C\Big)^{\frac{\Phi(Q_i)}{q-1}} \cdot a^{q-1} = (-1)^{d_i} a^{q-1}.$$

这表明 $((-1)^{d_i} Q_i)^{\frac{1}{q-1}} \in P$ $(1 \leqslant i \leqslant g)$. 由此可知

$$\mathcal{V} \subseteq \ker(l) \cap P.$$

反之,若 $\alpha \in \ker(l) \cap P$,则对每个 $\sigma \in G$, $\alpha^{\sigma-1} \in C$, $l(\alpha^{\sigma-1}) = 0$. 于是 $\alpha^{\sigma-1} \in \ker(l) \cap C = F_q^*$. 所以 $(\alpha^{q-1})^{\sigma-1} = 1$(对每个 $\sigma \in G$),即 $\alpha^{q-1} = g(T) \in k^*$. 又因为

$$g(T)^{\Phi(M)} = (\alpha^{s(G)})^{q-1} \in P^{s(G)(q-1)},$$

根据引理 2.3.2,便知有理函数 $g(T)$ 的分解式中只包含 Q_i $(1 \leqslant i \leqslant g)$,即 $g(T) = \prod_{i=1}^{g} Q_i^{k_i}$,其中 $k_i \in \mathbf{Z}$. 由 $l(\alpha) = 0$ 可知 $v_\infty(g(T)) = 0$,即 $\sum_{i=1}^{g} d_i k_i = 0$. 这表明 $\alpha \in \mathcal{V}$. ▌

引理 2.3.3 表明有群同构 $l: U/C \to l(U)/l(C)$. 因此

$$[U:C] = [l(U):l(C)]. \tag{2.3.1}$$

现在对每个 $\chi \in \hat{G}$,记本原幂等元为

$$e_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma) \sigma^{-1} \in \mathbf{C}[G].$$

特别地,对 G 的平凡特征 $\chi = \chi_0$,我们把 e_{χ_0} 记为

$$e_1 = \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1} = \frac{1}{|G|} s(G).$$

对于每个 $\mathbf{Z}[G]$-模 A,如下定义它的两个子模:

$A_0 = \{a \in A : s(G)x = 0\}$，$A^G = \{a \in A : ga = a, \forall g \in G\}$.
最后，我们用 $\langle X_1, \cdots, X_n\rangle$ 表示由 $X_1, \cdots, X_n$ 生成的阿贝尔群. 为了计算 $[l(U):l(C)]$，考虑图表(图 2.1)，其中 $T_1 = l(P)$ （自然看成为 $\boldsymbol{Q}[G]$-模）：

$$T_0 = \{x \in T_1 : s(G)x = 0\} \supseteq l(C).$$

而 $T_0 \subseteq (1-e_1)T_1$ 是根据于下面的引理：

引理 2.3.4　$T_0 = T_1 \cap (1-e_1)T_1$，并且

$$[(1-e_1)T_1 : T_0] = [I_1 : I_2],$$

其中 I_1 和 I_2 分别是 $\boldsymbol{Q}$ 的如下加法子群：

$$I_1 = (q-1)\left\langle \frac{d_1}{\Phi(Q_1^{c_1})}, \cdots, \frac{d_g}{\Phi(Q_g^{c_g})} \right\rangle;$$

$$I_2 = \langle d_1, \cdots, d_g \rangle.$$

$(1-e_1)T_1$　　$T_1 = l(P)$
T_0
$l(C)$

图　2.1

证明　由 $e_1 = \frac{1}{|G|}s(G)$ 易知 $T_0 = T_1 \cap (1-e_1)T_1$，于是

$$\frac{(1-e_1)T_1}{T_0} \cong \frac{T_1 + (1-e_1)T_1}{T_1} = \frac{T_1 + e_1T_1}{T_1}$$

$$\cong \frac{e_1T_1}{e_1T_1 \cap T_1} = \frac{e_1T_1}{T_1^G}.$$

由引理 2.3.2 可知

$$e_1T_1 = \frac{s(G)}{|G|}l(P) = \frac{1}{\Phi(M)}l(P^{s(G)})$$

$$= (q-1)\left(\sum_{i=1}^{g} \frac{d_i}{\Phi(Q_i^{c_i})}\mathbf{Z}\right)s(G) = I_1 s(G).$$

另一方面，对每个 $c \in P$，有

$$l(c) \in T_1^G \Leftrightarrow (\sigma - 1)l(c) = 0 \quad (\forall \sigma \in G)$$

$$\Leftrightarrow c^{\sigma-1} \in \boldsymbol{F}_q^* \quad (\forall \sigma \in G) \quad (\text{由引理 } 2.3.3(1))$$

$$\Leftrightarrow c^{q-1} \in k^* \Leftrightarrow c^{s(J)} \in k^*.$$

令 $P_1 = \{c \in P : c^{s(J)} \in k^*\}$，则 $l(P_1) = T_1^G$. 记 $\mathscr{M} = \langle Q_1, \cdots, Q_g\rangle$ 为 k^* 的乘法子群. 对每个 $Q = Q_i$，记 $e = e_i$，$H = \mathrm{Gal}(k(\Lambda_{Q^c})/k)$. 则对于本原 Q^c-torsion 元素 μ，$\mu^{s(H)} = Q$. 由于 $s(H) = s(J)\gamma$，$\gamma \in$

$\mathbf{Z}[H]$，所以 $Q=(\mu^J)^{s(J)}\in P_1^{s(J)}$. 这表明 $\mathscr{M}\subseteq P_1^{s(J)}$. 另一方面，由于 P_1 的 torsion 部分为 $\boldsymbol{F}_q^*$，可知 $P_1^{s(J)}$ 以及 $P_1^{s(J)}/\mathscr{M}$ 是 torsion-free 的. 再由

$$(P_1^{s(J)})^{\Phi(M)} = P_1^{s(J)s(G)} \subsetneq P_1^{s(J)} \subseteq \mathscr{M},$$

便知 $P_1^{s(J)}\subseteq\mathscr{M}$，即 $P_1^{s(J)}=\mathscr{M}$. 于是

$$T_1^{e_q} = l(P_1) = \frac{1}{q-1}l(P_1^{s(J)}) = \frac{1}{q-1}l(\mathscr{M})$$

$$= \Big(\sum_{i=1}^{g} d_i\mathbf{Z}\Big)s(G) = I_2 s(G).$$

这就完成了引理 2.3.4 的证明.　　■

现在我们计算$[(1-e_1)T_1:l(C)]$. 对每个 $x\in P$，$\sigma\in G$，则 $x^{\sigma-1}\in C$. 于是

$$\sigma l(x)\equiv l(x)\pmod{l(C)},$$

$$s(G)l(x)\equiv \Phi(M)l(x)\pmod{l(C)}.$$

如果 $l(x)\in T_0$，则 $\Phi(M)l(x)\in l(C)$. 这表明 $\Phi(M)$将 $T_0/l(C)$零化了. 所以$[T_0:l(C)]$有限，从而

$$[(1-e_1)T_1:l(C)] = [(1-e_1)T_1:T_0][T_0:l(C)]$$

也有限.

P 中每个元素表示成

$$x = \alpha\prod_{\lambda\in\Lambda_M^*}\lambda^{a_\lambda}\quad (a_\lambda\in\mathbf{Z})\quad \alpha\in\boldsymbol{F}_q^*.$$

进而，每个 $\lambda\in\Lambda_M^*$ 又可表成 $\lambda=\mu_1\cdots\mu_g$，其中 μ_i 是 $Q_i^{r_i}$ torsion 元素. 以 λ_i 表示取定的一个本原 $Q_i^{r_i}$-torsion 元素 $(1\leqslant i\leqslant g)$. 则

$$u^{Q_i^{r_i}} - \lambda_i^{Q_i^{r_i}} = \prod_{\deg A<\deg Q_i^{r_i}}\left(u-\lambda_i^{Q_i^{r_i-1}A+1}\right),$$

令 $u=0$，可知每个 $Q_i^{r_i}$-torsion 元素 μ_i 都是本原 $Q_i^{r_i}$-torsion 元素的积. 又对每个本原 $Q_i^{r_i}$-torsion 元素 λ_i'，$\lambda_i'/\lambda_i\in C$. 于是 P 中每个元素 x 最后可表示成

$$x = c\cdot\prod_{i=1}^{g}\lambda_i^{t_i}\quad (c\in C).$$

于是

$$l(x)\equiv\sum_{i=1}^{g}k_i l(\lambda_i)\pmod{l(C)}\quad(k_i\in\mathbf{Z},1\leqslant i\leqslant g).$$

引理 2.3.5 (1) 对每个 $x\in P$，$x=c\prod_{i=1}^{g}\lambda_i^{k_i}$ $(c\in C)$，我们有

$$l(x)\in T_0\Leftrightarrow\sum_{i=1}^{g}k_i d_i/\Phi(Q_i^{e_i})=0,$$

$$l(x)\in l(C)\Leftrightarrow\sum_{i=1}^{g}k_i d_i/\Phi(Q_i^{e_i})=0$$

并且 $$\Phi(Q_i^{e_i})\mid k_i(q-1)\quad(1\leqslant i\leqslant g).$$

(2) $[(1-e_1)T_1:l(C)]=\Phi(M)/(q-1)^g$.

证明 (1) 由于 $l(C)\subseteq T_0$，可知($M_i=M/Q_i^{e_i}$)：

$$s(G)l(x)=\sum_{i=1}^{g}k_i s(G)l(\lambda_i)=\sum_{i=1}^{g}k_i\Phi(M_i)l(Q_i).$$

因此

$$l(x)\in T_0\Leftrightarrow s(G)l(x)=0$$

$$\Leftrightarrow l(f)=0,\text{其中 } f=\prod_{i=1}^{g}Q_i^{\Phi(M_i)k_i}$$

$$\Leftrightarrow\deg f=0\Leftrightarrow\sum_{i=1}^{g}k_i d_i/\Phi(Q_i^{e_i})=0.$$

另一方面，

$$l(x)\in l(C)\Leftrightarrow\text{有 } c\in C,\text{使得 } l\Big(\prod_{i=1}^{g}\lambda_i^{k_i}\Big)=l(c)$$

$$\Leftrightarrow\prod_{i=1}^{g}\lambda_i^{k_i}=cy\quad(c\in C,y\in N)$$

$$\Leftrightarrow\prod_{i=1}^{g}\lambda_i^{k_i}=c\Big(\prod_{i=1}^{g}Q_i^{a_i}\Big)^{\frac{1}{q-1}}\quad(c\in C,a_i\in\mathbf{Z})$$

(由引理 2.3.3).

如果上式右端成立，取 $\mathscr{D}$ 为 $k(\Lambda_M)$ 中素除子，$\mathscr{D}\mid Q_i$，则

$$v_{\mathscr{D}}\Big(\prod_{i=1}^{g}\lambda_i^{k_i}\Big)=v_{\mathscr{D}}(\lambda_i^{k_i})=k_i,$$

$$v_{Q_i}\left(c\left(\prod Q_i^{a_i}\right)^{\frac{1}{q-1}}\right)=\frac{a_i}{q-1}v_{Q_i}(Q_i)=\frac{a_i\Phi(Q_i)}{q-1}.$$

这就表明 $\Phi(Q_i)\mid k_i(q-1)$ $(1\leqslant i\leqslant g)$，并且由 $l(x)\in T_0$ 可知 $\sum_{i=1}^{g}k_id_i/\Phi(Q_i)=0$. 反之，若 $l(x)\in T_0$，并且 $\Phi(Q_i)\mid k_i(q-1)$ $(1\leqslant i\leqslant g)$，则 $a_i=k_i(q-1)/\Phi(Q_i)\in\mathbf{Z}$ $(1\leqslant i\leqslant g)$，并且

$$v_\infty\left(\prod Q_i^{a_i}\right)=\sum a_id_i=(q-1)\sum k_id_i/\Phi(Q_i)=0.$$

因此 $\prod Q_i^{a_i}\in N$，于是

$$l(x)\equiv\sum k_il(\lambda_i)\pmod{l(C)}$$

$$=\sum a_il\left(\lambda_i^{\Phi(Q_i)/(q-1)}\right)\equiv l\left(\prod Q_i^{a_i/(q-1)}\right)\equiv 0\pmod{l(C)}.$$

即 $l(x)\in l(C)$. 这就表明了：

$l(x)\in l(C)\Leftrightarrow\sum_{i=1}^{g}k_id_i/\Phi(Q_i)=0$，并且 $\Phi(Q_i)\mid k_i(q-1)$ $(1\leqslant i\leqslant g)$.

(2) 定义 $\mathbf{R}^g$ 中两个格：

$$L_1=\{(y_1,\cdots,y_g):y_i\in\frac{(q-1)d_i}{\Phi(Q_i)}\mathbf{Z}\},$$

$$L_2=\{(y_1,\cdots,y_g):y_i\in d_i\mathbf{Z}\}\subseteq L_1.$$

并且考虑加法群同态：

$$\Psi:L_1\to\mathbf{R},\quad \Psi(y_1,y_2,\cdots,y_g)=y_1+y_2+\cdots+y_g,$$

则根据引理2.3.4，有

$$\Psi(L_1)/\Psi(L_2)\cong I_1/I_2\cong e_1T_1/T_1^{G}\cong(1-e_1)T_1/T_0.$$

另一方面，记 K_1、K_2分别为 Ψ 在 L_1和 L_2中的核，由(1)中所证又知道$[T_0:l(C)]=[K_1:K_2]$. 于是

$$\Phi(M)/(q-1)^g=[L_1:L_2]=[\Psi(L_1):\Psi(L_2)][K_1:K_2]$$

$$=[(1-e_1)T_1:T_0][T_0:l(C)]$$

$$=[(1-e_1)T_1:l(C)].$$

这就完成了引理2.3.5的证明. ∎

于是，为了计算$[U:C]=[l(U):l(C)]$，我们只需计算$[l(U):$

$(1-e_1)T_1]$. 为此，我们需要研究$(1-e_1)T_1$的 $\mathbf{Z}[G]$-模结构. 现在仍固定 $K=k(\Lambda_M)$的一个无限素除子 $\mathscr{P}$. 于是有本原 M-torsion 元素 λ，使得对每个 $A\in R$，$\deg A<d$，均有$(d=\deg M)$：

$$v_{\mathscr{P}}(\lambda^A)=m(A)=(q-1)(d-\deg A-1)-1.$$

将每个 $\chi\in\hat{G}$ 看成模 M 的特征，其中 $G=G(K/k)\cong(R/(M))^*$. 如前一样，以 χ^* 表示与 χ 相结合的本原特征，F_χ 为 χ 的导子. 定义

$$\phi(\chi)=\sum_{A\in(R/(F_\chi))^*}m(A)\chi^*(A)\in\mathbf{C}.$$

则当 χ 不是实特征时，由 $m(A)$的定义可知 $\phi(\chi)=0$. 又令

$$\omega=\sum_{\chi_0\neq\chi\in\hat{G}}\phi(\bar{\chi})e_\chi=\sum_{\chi_0\neq\chi\in\hat{G}^-}\phi(\bar{\chi})e_\chi\in\mathbf{C}[G].$$

对于 $M\nmid A$，记

$$\eta(A)=l(\lambda^A)=\sum_{B\in(R/(M))^*}m(AB)\sigma_B^{-1},$$

则当$(C,M)=1$时，$\sigma_C(\eta(A))=\eta(AC)$. 于是 $T_1=l(P)$就是由$\{\eta(A):A\in R,M\nmid A\}$生成的加法子群. 进而，对每一个 $F|M$，记

$$H_F=\{\sigma_A\in G:A\equiv 1\pmod F\}=\mathrm{Gal}(k(\Lambda_M)/k(\Lambda_F)).$$

对 $R=\mathbf{F}_q[T]$中每一个首1不可约多项式 Q，定义

$$\bar{\sigma}_Q=\sum_{\chi\in\hat{G}}\bar{\chi}^*(Q)e_\chi\in\mathbf{Q}[G],$$

则对每一个 $\chi\in\hat{G}$，$\chi^*(\bar{\sigma}_Q)=\bar{\chi}^*(Q)$. 我们以 W 表示 $\mathbf{Q}[G]$中由

$$\{s(H_F)\prod_{Q|F}(1-\bar{\sigma}_Q):F|M\}$$

生成的 $\mathbf{Z}[G]$-模.

引理2.3.6 (1) $(1-e_1)T_1=\omega W$.

(2) 有阿贝尔群同构 $W\cong\mathbf{Z}^{\Phi(M)}$.

证明 (1) 设 $M=AF$，我们只需证明

$$(1-e_1)\eta(A)=\omega s(H_F)\prod_{Q|F}(1-\bar{\sigma}_Q).\qquad(2.3.2)$$

这只需对每个 $\chi\in\hat{G}$，证明 χ^* 在上式两端的取值相等即可. 若 $\chi=\chi_0$，或者 $\chi(\mathbf{F}_q^*)\neq1$，或者 $F_\chi\nmid F$，则 χ^*(左)$=0$. 另一方面，若 χ

$=\chi_0$或者 $\chi(F_q^*)\neq 1$,则 $\chi^*(\omega)=0$. 若 $F_\chi\nmid F$,则 $\chi^*(s(H_F))=0$. 所以也有 χ^*(右)$=0$. 现在设 $\chi_0\neq\chi\in\hat{G}^{+}$,并且 $F_\chi|F$. 这时

$$\chi^*(\text{左})=\frac{\Phi(M)}{\Phi(F)}\sum_{B\in(R/(F))^*}m(AB)\bar{\chi}^*(B)$$

$$=\frac{\Phi(M)}{\Phi(F)}\sum_{B\in(R/(F))^*}m(B)\bar{\chi}^*(B)$$

(由 $m(B)$ 的定义和 $\chi\neq\chi_0$),

$$\chi^*(\text{右})=\sum_{A\in(R/(F_\chi))^*}m(A)\bar{\chi}^*(A)\cdot\frac{\Phi(M)}{\Phi(F)}\cdot\prod_{Q|F}(1-\bar{\chi}^*(Q)).$$

$$=\chi^*(\text{左})\quad(\text{引理 } 2.1.3)$$

这就表明(2.3.2)式成立,于是$(1-e_1)T_1=\omega W$.

(2) 对于每个首1不可约多项式 $Q\in F_q[T]$,我们以 W_Q 表示 $Q[G]$中由 $s(T_Q)$和$(1-\bar{\sigma}_Q)$生成的 $\mathbf{Z}[G]$-子模,其中

$$T_Q=H_{M/Q'},\quad Q'\|M.$$

现在证明:作为阿贝尔群,有

$$W=\prod_{Q|M}W_Q,\tag{2.3.3}$$

记上式右端为 W'. 由于

$$G=\mathrm{Gal}(k(\Lambda_M)/k)=\prod_{Q|M}T_Q\quad(\text{直积}).$$

所以作为 $\mathbf{Z}[G]$-模,W'是由

$$\prod_{Q\in S}s(T_Q)\prod_{\substack{Q\notin S\\Q|M}}(1-\bar{\sigma}_Q)\tag{2.3.4}$$

生成的,其中 S 过$\{Q:Q|M\}$的全部子集. 对于每个 S,对应地有分解:

$$M=FA,\ (F,A)=1,\ S=\{Q:Q|A\}.$$

由于$\prod_{Q|A}T_Q=H_F$, 所以

$$\prod_{Q\in S}s(T_Q)=\prod_{Q|A}s(T_Q)=s(H_F).$$

于是(2.3.4)式等于 $s(H_F)\prod_{Q|F}(1-\bar{\sigma}_Q)\in W$. 这就表明 $W'\subseteq W$. 另

一方面，$\boldsymbol{Z}[G]$-模 W 是由

$$s(H_F)\prod_{Q|F}(1-\bar{\sigma}_Q) \tag{2.3.5}$$

生成的，其中 F 过 M 的所有首1因子. 对每个这样的 F，令 $S=\{Q:Q|M,Q\nmid F\}$，则 $\prod_{Q\in S}T_Q$ 是 H_F 的子群. 于是有 $\beta\in\boldsymbol{Z}[G]$，使得

$$s(H_F)=\beta\cdot s\Big(\prod_{Q\in S}T_Q\Big)=\beta\prod_{Q\in S}s(T_Q).$$

而 $\prod_{Q|F}(1-\bar{\sigma}_Q)=\prod_{\substack{Q|M\\ Q\notin S}}(1-\bar{\sigma}_Q)$. 所以(2.3.5)式等于

$$\beta\prod_{Q\in S}s(T_Q)\prod_{\substack{Q|M\\ Q\notin S}}(1-\bar{\sigma}_Q)\in W'.$$

这就表明 $W\subseteq W'$. 于是 $W=W'$，即(2.3.3)式成立.

现在对每个 $Q|M$，我们证明阿贝尔群 W_Q 都同构于 $\boldsymbol{Z}^{\Phi(M)}$. 为此，令 $e_Q=s(T_Q)/|T_Q|$. 则对每个 $\chi\in\hat{G}$，有

$$\chi(e_Q)=\begin{cases}1, & 若\ Q\nmid F_\chi;\\ 0, & 若\ Q|F_\chi.\end{cases}$$

设 $Q^r\|M$，并取 $N\in\boldsymbol{F}_q[T]$满足

$$N\equiv1\pmod{Q^r},\quad N\equiv Q\pmod{M/Q^r}.$$

记 $\lambda_Q=\sigma_N$，则对每个 $\chi\in\hat{G}$，$\chi(\lambda_Q^{-1}e_Q)=\bar{\chi}(Q)$. 于是 $\bar{\sigma}_Q=\lambda_Q^{-1}e_Q\in\boldsymbol{Q}[G]$. 所以

$$|T_Q|=\lambda_Q^{-1}s(T_Q)+|T_Q|(1-\bar{\sigma}_Q)\in W_Q.$$

由于 W_Q 是 $\boldsymbol{Q}[G]$中有限生成的 $\boldsymbol{Z}[G]$-模，并且 $|T_Q|\in W_Q$，可知

$$W_Q\cong\boldsymbol{Z}^{\Phi(M)}.$$

最后，W 是 $\boldsymbol{Q}[G]$中有限生成的 $\boldsymbol{Z}[G]$-模，并且 $\prod_{Q|M}|T_Q|\in W$，可知 $W\cong\boldsymbol{Z}^{\Phi(N)}$. 这就证明了引理2.3.6. ▍

定理2.3.7　设 $k=\boldsymbol{F}_q(T)$，$K=k(\Lambda_M)$，则

$$[U_K:C]=h(O_K^+)\Phi(M)Q_0(q-1)^{-g}[e^+\boldsymbol{Z}[G]_0:e^+W_0],$$

其中 g 为 M 中不同的首1不可约因子的个数，$e^+=\frac{s(J)}{q-1}$，$Q_0=[U_K:U_K^+]$(其值由引理1.2.6算出)，而对每个 $\boldsymbol{Z}[G]$-模 A，令 $A_0=\{a\in A:s(G)a=0\}$.

证明　我们有

$$[U_K:C]=[l(U_K):l(C)]$$
$$=[l(U_K):e^+\mathbf{Z}[G]_0][e^+\mathbf{Z}[G]_0:e^+W_0]$$
$$\times[e^+W_0:(1-e_1)T_1][(1-e_1)T_1:l(C)].$$

我们已经算出$[(1-e_1)T_1:l(C)]=(q-1)^{-g}\Phi(M)$（引理2.3.5）.
下面要计算出：

(1) $[l(U_K):e^+\mathbf{Z}[G]_0]=Q_0/R(O_K^+)(q-1)^{2r}$，$r=\dfrac{\Phi(M)}{q-1}-1$.

(2) $[e^+W_0:(1-e_1)T_1]=(q-1)^{2r}h(K^+)$.

由此即得定理2.3.7.

(1) $l(U_K)$和$l(C)$都是r维$\mathbf{Q}$-向量空间$X=(1-e_1)e^+\mathbf{Q}[G]$的加法子群. 而$e^+\mathbf{Z}[G]_0$是$X$中的格，它有$\mathbf{Z}$-基：

$$\{e^+(\sigma_A-1):A\in R_1,\ 1\leqslant \deg A<\deg M,\ (A,M)=1\}.$$

另一方面，设$\eta_1,\cdots,\eta_r$是U_K的一组基本单位系，则

$$l(\eta_i)=\sum_{1\neq A\in(R/(M))^*}v_{\mathfrak{P}_A}(\eta_i)(\sigma_A^{-1}-1)$$
$$=(q-1)\sum_{\substack{(A,M)=1\\ A\in R_1\\ 1\leqslant\deg A<\deg M}}v_{\mathfrak{P}_A}(\eta_i)e^+(\sigma_A^{-1}-1).$$

但是

$$\det(v_{\mathfrak{P}_A}(\eta_i))=R(O_K)=R(O_K^+)(q-1)^r/Q_0\quad(\text{引理 }1.3.2).$$

这就表明

$$[l(U_K):e^+\mathbf{Z}[G]_0]=(q-1)^r\det(v_{\mathfrak{P}_A}(\eta_i))^{-1}$$
$$=Q_0/R(O_K^+)(q-1)^{2r}.$$

(2) 由引理2.3.6知道$(1-e_1)T_1=\omega W$. 由$T_1=l(P)$可知$(1-e_1)T_1\subseteq X$. 而对每个$x\in X$，$(1-e_1)e^+x=x$. 于是

$$(1-e_1)T_1=\omega e^+(1-e_1)W=\omega e^+W_0.$$

定义线性映射：$f:X\to X$，$f(x)=\omega x$.
则$f(e^+W_0)=(1-e_1)T_1$. 由ω的定义可知

$$[e^+W_0:(1-e_1)T_1]=\det(f)=\prod_{\chi_0\neq\chi\in\hat{G}^+}\phi(\chi)$$

$$= (q-1)^r \prod_{\chi_0\neq\chi\in\hat{G}^+} \Big(\sum_{\substack{A\in R_1\\(A,M)=1\\ \deg A<\deg M}} m(A)\chi^*(A)\Big)$$

$$= (q-1)^{2r}h(K^+). \quad \blacksquare$$

§ 2.4　计算$[e^+\mathbf{Z}[G]_0:e^+W_0]$

在本节中，我们完成定理2.3.1的证明. 由定理2.3.7归结于计算$[e^+\mathbf{Z}[G]_0:e^+W_0]$. 其中

$$e^+ = (q-1)^{-1}s(J),\quad s(J) = \sum_{a\in F_q^*}\sigma_a,$$

$$\mathbf{Z}[G]_0 = \{\alpha\in\mathbf{Z}[G]: s(G)\alpha = 0\},$$

$$W = \prod_{Q|M} W_Q,\quad W_0 = \{\alpha\in W: s(G)\alpha = 0\},$$

$$W_Q = s(T_Q)\mathbf{Z}[G] + (1-\bar{\sigma}_Q)\mathbf{Z}[G] \subseteq \mathbf{Q}[G],$$

$$\bar{\sigma}_Q = \sum_{\chi\in\hat{G}}\bar{\chi}^*(Q)e_\chi \in \mathbf{Q}[G],$$

$$T_Q = \{\sigma_A: A\in R, A\equiv 1 \pmod{M/Q^r}\}\quad (Q^r\|M).$$

由引理2.3.6的证明知道，取$N\in R$满足

$$N\equiv 1 \pmod{Q^r},\quad N\equiv Q \pmod{M/Q^r},$$

并令$\lambda_Q=\sigma_N$，则$\bar{\sigma}_Q=\lambda_Q^{-1}e_Q$.

本节的主要任务是证明如下定理：

定理2.4.1　设g为M的不同首1不可约因子的个数. 则

$$[e^+\mathbf{Z}[G]_0:e^+W_0] = \begin{cases}(q-1)/\Phi(M), & 若\ g=1;\\ (q-1)^{2^{g-2}}/\Phi(M), & 若\ g\geqslant 2.\end{cases}$$

由此及定理2.3.7和Q_0的值（引理1.2.6）即得定理2.3.1. 为了证明定理2.4.1，需要研究$\mathbf{Z}[G]$-模W_Q的更加精细的结构，记

$$M=\prod_{i=1}^{g}Q_i^{r_i},\quad \bar{M}=Q_1Q_2\cdots Q_g.$$

对于$\bar{M}$的每个首1因子S，令

$$W_S=\prod_{Q|S}W_Q, T_S=\prod_{Q|S}T_Q.$$

于是 $W_1=\mathbf{Z}[G]$，$W_{\bar{M}}=W$，$T_1=\{1\}$，$T_{\bar{M}}=G$.

现在设 $rQ|\bar{M}$. 由于 e_Q 是幂等元，所以 $(1-e_Q)s(T_Q)=0$. 于是

$$(1-e_Q)(1-\bar{\sigma}_Q)=(1-e_Q)(1-\lambda_Q^{-1}e_Q)=(1-e_Q).$$

因此

$$\begin{aligned}(1-e_Q)W_{rQ}&=(1-e_Q)W_QW_r\\&=(1-e_Q)[s(T_Q)\mathbf{Z}[G]+(1-\bar{\sigma}_Q)\mathbf{Z}[G]]W_r\\&=(1-e_Q)W_r.\end{aligned}$$

易知满同态

$$W\to(1-e_Q)W,\quad \alpha\mapsto(1-e_Q)\alpha$$

的核为

$$W^{T_Q}=\{\alpha\in W:\sigma(\alpha)=\alpha\text{ 对每个 }\sigma\in T_Q\}.$$

于是有行正合 $\mathbf{Z}[G]$-模图表(图2.2)如下：

$$\begin{array}{ll}0\to W_r^{T_Q}\to W_r\to(1-e_Q)W_r\to 0 & \text{(正合)}\\ \qquad\qquad\qquad\qquad\quad\| & \\ 0\to W_{rQ}^{T_Q}\to W_{rQ}\to(1-e_Q)W_{rQ}\to 0 & \text{(正合)}\end{array}$$

图　2.2

引理2.4.2　(1) 设 $Q|\bar{M}$，H 为 G 的子群，$H\cap T_Q=\{1\}$. 如果 A 为 $\mathbf{Q}[G]$ 的自由 $\mathbf{Z}[HT_Q]$-子模，则 A^{T_Q} 和 $(1-e_Q)A$ 都是自由 $\mathbf{Z}[H]$-模.

(2) 若 $rQ|\bar{M}$，则 $W_{rQ}^{T_Q}=s(T_Q)W_r+(1-\lambda_Q^{-1})W_r^{T_Q}$.

证明　(1) 不妨设 $A=\mathbf{Z}[HT_Q]$，因为在一般情形下，A 是一些 $\mathbf{Z}[HT_Q]$ 的直和. 于是有直和分解

$$A=B+C,$$

其中

$$B=s(T_Q)\mathbf{Z}[H]=A^{T_Q},$$

$$C=\Big(\sum_{1\neq\tau\in T_Q}\tau\Big)\mathbf{Z}[H]=A/A^{T_Q}\cong(1-e_Q)A,$$

都是自由 $\mathbf{Z}[H]$-模.

(2) 由 $W_{rQ}=W_QW_r=s(T_Q)W_r+(1-\bar{\sigma}_Q)W_r$ 可知 W_{rQ} 中的元

素均可以表示成：

$$x = s(T_Q)y + (1-\bar{\sigma}_Q)z, \quad y,z \in W_r.$$

于是

$$x \in W_{rQ}^{T_Q} \Longleftrightarrow (1-e_Q)x = 0 \Longleftrightarrow (1-e_Q)z = 0 \Longleftrightarrow z \in W_r^{T_Q}.$$

这表明 $W_{rQ}^{T_Q}=s(T_Q)W_r+(1-\bar{\sigma}_Q)W_r^{T_Q}$. 进而当 $z\in W_r^{T_Q}$ 时，$e_Qz=z$，于是 $(1-\bar{\sigma}_Q)z=(1-\lambda_Q^{-1}e_Q)z=(1-\lambda_Q^{-1})z$. 这就证明了(2). ▌

现在考虑 $k=\boldsymbol{F}_q(T)$ 中无限素除子 $\infty=\left(\frac{1}{T}\right)$ 的惰性群 $T_\infty=J$. 对于每个首1多项式 $r\mid\bar{M}, r\neq\bar{M}$，则 $J\cap T_r=\{1\}$.

引理2.4.3 设 $rr'\mid\bar{M}$. 则 W_r 是自由 $T_{r'}$-模，并且当 $rr'\neq\bar{M}$ 时，W_r 为自由 $T_\infty T_{r'}$-模(今后对 G 的每个子群 H，$\mathbf{Z}[H]$-模也称作 H-模).

证明 我们对 r 的首 1 不可约因子的个数进行归纳. 当 $r=1$ 时引理成立，因为 $W_1=\mathbf{Z}[G]$，而对 G 的每个子群 H，$\mathbf{Z}[G]$为自由 H-模. 现在设引理对 r 成立. 令 $rQ\mid\bar{M}$，只需再证引理对 rQ 也成立即可. 设 $rQr'\mid\bar{M}$. 由归纳假设知 W_r 为自由 $T_{r'Q}$-模. 由于 $T_{r'}\cap T_Q=\{1\}$，引理2.4.2的(1)表明 $W_r^{T_Q}$ 和 $(1-e_Q)W_r$ 都是自由 $T_{r'}$-模. 图2.2给出了 $T_{r'}$-模同构：

$$W_{rQ} \cong W_{rQ}^{T_Q} \oplus (1-e_Q)W_r.$$

另一方面，引理2.4.2的(2)给出了

$$W_{rQ}^{T_Q} = s(Q)W_r + (1-\lambda_Q^{-1})W_r^{T_Q}.$$

由归纳假设知 W_r 为自由 T_Q-模，因此 $s(T_Q)W_r=W_r^{T_Q}$. 于是 $W_{rQ}=W_r^{T_Q}\oplus(1-e_Q)W_r$. 由上述右端的两个模均是自由 $T_{r'}$-模，所以 W_{rQ} 也是如此.

又设 $rQr'\neq\bar{M}$. 由归纳假设知 W_r 是自由 $T_\infty T_{r'Q}$-模. 由引理2.4.2知 $W_r^{T_Q}$ 和 $(1-e_Q)W_r$ 均是自由 $T_\infty T_{r'}$-模，于是 W_{rQ}也是如此. ▌

接下来我们需要计算一些有限群的上同调群. 设 G 是有限群，A 为 G-模(即是 $\mathbf{Z}[G]$-模). 我们只用到上同调群的如下性质(这些性质可参见任何一本讲述有限群的上同调的书)：

引理2.4.4　(1) $H^0(G,A)=A^G$，又若 A 是自由 G-模，则当 $n\geqslant1$时，$H^n(G,A)=(0)$.

(2) 若 G 是由 σ 生成的 m 阶循环群，A 为 G-模，$N=s(G)$. 则当 $l\geqslant1$时，

$$H^{2l}(G,A)=A^G/N(A),\quad H^{2l-1}(G,A)=A_N/(1-\sigma)A,$$

其中 $A_N=\{a\in A;Na=0\}$.

(3) 设 A 是 G-模，H 为 G 的正规子群，则有群正合序列

$$0\to H^1(G/H,A^H)\xrightarrow{\inf}H^1(G,A)\xrightarrow{\text{res}}H^1(H,A).$$

更一般地，如果 $H^i(H,A)=0$ $(1\leqslant i\leqslant m-1)$，则有群正合序列

$$0\to H^m(G/H,A^H)\xrightarrow{\inf}H^m(G,A)\xrightarrow{\text{res}}H^m(H,A).$$

(4) 若$0\to B\to A\to C\to0$是 G-模正合序列，则有长正合序列

$$H^0(G,B)\to H^0(G,A)\to H^0(G,C)\to H^1(G,B)\to\cdots$$
$$\to H^m(G,B)\to H^m(G,A)\to H^m(G,C)\to H^{m+1}(G,B)\to\cdots.$$

最后，若 G 是有限阿贝尔群，则 $H^m(G,A)$有自然的 G-模结构，并且(4) 中同态和正合序列均是 G-模同态和正合序列.

现在我们来计算一些上同调群：

引理2.4.5　设 $rr'|\overline{M}$，$\deg r\geqslant1$，$\deg r'\geqslant1$. 则对每个 $m\geqslant1$有群同构

$$H^m(T_{r'},W_r^{T_\infty})\cong H^m(T_\infty T_{r'},W_r)\cong H^m(T_\infty,W_r^{T_{r'}}),$$

并且若 $rr'\neq\overline{M}$，则上面三个群均为(0).

证明　由假设可知 $r\neq\overline{M}$，于是 W_r 是自由 T_∞-模（引理2.4.3），所以对每个 $m\geqslant1$，$H^m(T_\infty,W_r)=(0)$（引理2.4.4(1)）. 再由引理2.4.4(3)可知

$$H^m(T_\infty T_{r'}/T_\infty,W_r^{T_\infty})\cong H^m(T_\infty T_{r'},W_r)\quad(m\geqslant1).$$

由 $r'\neq\overline{M}$ 知 $T_\infty T_{r'}=T_\infty\times T_{r'}$（直积），可知 $T_\infty T_{r'}/T_\infty\cong T_{r'}$. 故上式左端可看成 $H^m(T_{r'},W_r^{T_\infty})$. 由引理2.4.3知 W_r 是自由$T_{r'}$-模，于是 $H^m(T_{r'},W_r)=(0)$ $(m\geqslant1)$. 再由引理2.4.4(3)得到

$$H^m(T_\infty,W_r^{T_{r'}})=H^m(T_\infty T_{r'}/T_{r'},W_r^{T_{r'}})\cong H^m(T_\infty T_{r'},W_r).$$

最后若 $rr'\neq\overline{M}$，则 W_r 是自由 $T_\infty T_{r'}$-模，所以 $H^m(T_\infty T_{r'},W_r)=$

(0). 这就证明了引理2.4.5. ▌

现在回到有限阿贝尔群：

$$G = \mathrm{Gal}(k(\Lambda_M)/k) \quad (k = \boldsymbol{F}_q(T))$$

和它的子群 $J = \{\sigma_a \in G : a \in \boldsymbol{F}_q^*\}$. 对于 $r'r = \overline{M}$, 定义

$$A_r^m = H^m(J, W_r^{T_{r'}}).$$

引理2.4.6　(1) 对每个 $m \geqslant 1$, $(q-1)A_r^m = (0)$, 并且 A_r^m 是平凡 G-模.

(2) 设 $Qr \mid \overline{M}$, 则对每个 $m \geqslant 1$ 都有群正合序列 $0 \to A_r^m \to A_{rQ}^m \to A_r^{m+1} \to 0$.

证明　(1) 以 σ 表示 J 的生成元, 则 $N = s(J) = 1 + \sigma + \sigma^2 + \cdots + \sigma^{q-2}$. 在引理2.4.4(2)中取 $A = W_r^{T_{r'}}$　$(rr' = \overline{M})$, 则对每个 $m \geqslant 1$, 有

$$H^{2m}(J, A) = A^J/NA, \quad H^{2m-1}(J, A) = A_N/(\sigma - 1)A,$$

易知 $(q-1)A^J \subseteq NA$, $(q-1)A_N \subseteq (\sigma - 1)A$. 所以对每个 $m \geqslant 1$, $(q-1)A_r^m = (0)$.

为证 A_r^m 是平凡 G-模, 只需对每个 $Q \mid \overline{M}$ 证明 A_r^m 是平凡 T_Q-模 $\left(\text{因为 } G = \coprod_{Q \mid \overline{M}} T_Q\right)$. 如果 $Q \mid r' = \overline{M}/r$, 由定义知 T_Q 在 $W_r^{T_{r'}}$ 上作用也平凡, 所以在 $A_r^m = H^m(J, W_r^{T_{r'}})$ 上作用平凡. 现在设 $Q \mid r$, 记 $r = SQ$. 则有

$$W_r = W_Q W_S = s(T_Q)W_S + (1 - \bar{\sigma}_Q)W_S.$$

对每个 $\tau \in T_Q$, 有

$$(\tau - 1)(1 - \bar{\sigma}_Q) = (\tau - 1)(1 - |T_Q|^{-1}\lambda_Q^{-1}s(TQ)) = \tau - 1.$$

于是 $(\tau - 1)W_r = (\tau - 1)W_S \subseteq W_S$. 我们有两个同态：

$$f: W_r \to W_S, x \mapsto (\tau - 1)x;$$

$$g: W_S \to W_r, x \mapsto (1 - \bar{\sigma}_Q)x.$$

并且有交换图表如图2.3. 由此得到交换图表如图2.4. 作用于 $H^m(J,)$ 之后, 得到交换图表如图2.5.

由于 $Sr' \neq \overline{M}$, 可知 $H^m(J, W_S^{T_{r'}}) = (0)$. 于是对每个 $\tau \in T_Q$, $(\tau - 1)(A_r^m) = (0)$, 即 A_r^m 是平凡 T_Q-模. 这就证明了(1).

（2）由图2.2给出了行正合的 G-模图表：

$$
\begin{array}{ccccccccc}
0 & \to & W_r^{T_Q} & \to & W_r & \to & (1-e_Q)W_r & \to & 0 \quad （正合）\\
 & & & & & & \| & & \\
0 & \to & W_{rQ}^{T_Q} & \to & W_{rQ} & \to & (1-e_Q)W_{rQ} & \to & 0 \quad （正合）
\end{array}
$$

图　2.2

$$
\begin{array}{ccc}
W_r & \xrightarrow{\tau-1} & W_r \\
 & {\scriptstyle f}\searrow \quad \nearrow{\scriptstyle g} & \\
 & W_S &
\end{array}
\qquad
\begin{array}{ccc}
W_r^{T_{r'}} & \xrightarrow{\tau-1} & W_r^{T_{r'}} \\
 & \searrow \quad \nearrow & \\
 & W_S^{T_{r'}} &
\end{array}
\qquad
\begin{array}{ccc}
A_r^m & \xrightarrow{\tau-1} & A_r^m \\
 & {\scriptstyle f^*}\searrow \quad \nearrow{\scriptstyle g^*} & \\
 & H^m(J, W_S^{T_{r'}}) &
\end{array}
$$

图　2.3　　　　图　2.4　　　　图　2.5

再考虑交换图表(图2.6)：

$$
\begin{array}{ccccc}
W_r & \xrightarrow{1-e_Q} & (1-e_Q)W_r & \to & 0 \\
{\scriptstyle 1-\bar{\sigma}_Q}\downarrow & & \| & & \\
W_{rQ} & \xrightarrow{1-e_Q} & (1-e_Q)W_{rQ} & \to & 0
\end{array}
$$

图　2.6

当 $x \in W_r^{T_Q}$ 时，$e_Q x = x$，从而$(1-\bar{\sigma}_Q)x = (1-\lambda_Q^{-1})x$. 于是上面的图2.2和图2.6给出了以下的行正合交换图表(图2.7)：

$$
\begin{array}{ccccccccc}
0 & \to & W_r^{T_Q} & \to & W_r & \to & (1-e_Q)W_r & \to & 0 \quad （正合）\\
 & & {\scriptstyle 1-\lambda_Q^{-1}}\downarrow & & \downarrow{\scriptstyle 1-\bar{\sigma}_Q} & & \| & & \\
0 & \to & W_r^{T_Q} & \to & W_{rQ} & \to & (1-e_Q)W_r & \to & 0 \quad （正合）
\end{array}
$$

图　2.7

(注意，引理2.4.3的证明中给出了 $W_{rQ}^{T_Q} = s(Q)W_r + (1-\lambda_Q^{-1})W_r^{T_Q}$ 和 $s(T_Q)W_r = W_r^{T_Q}$，于是 $W_{rQ}^{T_Q} = W_r^{T_Q}$.) 记 $rr'Q = \overline{M}$. 现在 W_{rQ}为自由 $T_{r'}$-模，W_r 为自由 $T_{r'Q}$-模，于是 $W_r^{T_Q}$，$(1-e_Q)W_r$，W_r，W_{rQ}均是自由 $T_{r'}$-模. 所以上面的交换图表给出了如下的行正合交换图表(图2.8)：

$$
\begin{array}{ccccccccc}
0 & \to & W_r^{T_{r'Q}} & \to & W_r^{T_{r'}} & \to & ((1-e_Q)W_r)^{T_{r'}} & \to & 0 \quad （正合）\\
 & & {\scriptstyle 1-\lambda_Q^{-1}}\downarrow & & \downarrow & & \| & & \\
0 & \to & W_r^{T_{r'Q}} & \to & W_{rQ}^{T_{r'}} & \to & ((1-e_Q)W_r)^{T_{r'}} & \to & 0 \quad （正合）
\end{array}
$$

图　2.8

记 $Y=((1-e_Q)W_r)^{T_{r'}}$，我们又有行正合的交换图表(图2.9)：

$$\begin{array}{ccccc}
\cdots\to H^{m-1}(J,Y) & \longrightarrow & A_r^m & \to & H^m(J,W_r^{T_{r'}}) \\
\| & & \downarrow 1-\lambda_Q^{-1} & & \downarrow \\
\cdots\to H^{m-1}(J,Y) & \xrightarrow{\alpha} & A_r^m & \longrightarrow & A_{rQ}^m \\
\to H^m(J,Y) & \longrightarrow & A_r^{m+1} & \to & H^{m+1}(J,W_r^{T_{r'}})\to\cdots \\
\| & & \downarrow 1-\lambda_Q^{-1} & & \downarrow \\
\to H^m(J,Y) & \xrightarrow{\beta} & A_r^{m+1} & \longrightarrow & A_{rQ}^{m+1}\to\cdots
\end{array}$$

图 2.9

由于 A_r^m 和 A_r^{m+1} 为平凡 G-模，所以

$$(1-\lambda_Q^{-1})A_r^m=(1-\lambda_Q^{-1})A_r^{m+1}=(0),\ 即\ \alpha=\beta=0.$$

于是有正合序列：

$$0\to A_r^m\to A_{rQ}^m\to H^m(J,Y)\to 0.$$

另一方面，$H^m(J,W_r^{T_{r'}})=(0)$，所以 $H^m(J,Y)\cong A_r^{m+1}$. 这就给出了正合序列$0\to A_r^m\to A_{rQ}^m\to A_r^{m+1}\to 0$. ▌

现在我们可以决定阿贝尔群 $A_r^m(m\geq 1)$的结构.

引理2.4.7 设 $m\geq 1$，$r\bar{r}=\bar{M}$，a 为 r 的首1不可约因子的个数，则 $a\geq 1$时，$A_r^m\cong(\mathbf{Z}/(q-1)\mathbf{Z})^{2^{a-1}}$. 而当 $a=0$(即 $r=1$)时，

$$A_1^m\cong\begin{cases}(0), & 若\ 2\nmid m;\\ \mathbf{Z}/(q-1)\mathbf{Z}, & 若\ 2\mid m.\end{cases}$$

证明 $W_1=\mathbf{Z}[G]$，$T_{\bar{M}}=G$，于是当$2\mid m$ 时，

$$\begin{aligned}A_1^m&=H^m(J,\mathbf{Z}[G]^G)=H^m(J,s(G)\mathbf{Z})\\&=s(G)\mathbf{Z}/s(J)s(G)\mathbf{Z}\\&=s(G)\mathbf{Z}/(q-1)s(G)\mathbf{Z}\cong\mathbf{Z}/(q-1)\mathbf{Z}.\end{aligned}$$

而当$2\nmid m$ 时，

$$A_1^m=(s(G)\mathbf{Z})_J/(1-\sigma)(s(G)\mathbf{Z})=(0).$$

进而，引理2.4.6给出了正合序列$0\to A_r^m\to A_{rQ}^m\to A_r^{m+1}\to 0$，其中$Qr\mid\bar{M}$. 于是 $A_{rQ}^m=A_r^m\times A_r^{m+1}$. 取 $r=1$，得 $A_Q^m\cong\mathbf{Z}/(q-1)\mathbf{Z}(m\geq 1)$. 然后用归纳法，可知 $A_r^m\cong(\mathbf{Z}/(q-1)\mathbf{Z})^{2^{a-1}}(m\geq 1)$. ▌

有了以上准备，我们现在证明定理2.4.1：

令 $\overline{M}=Q_1\cdots Q_g(g\geqslant 1)$，$s_0=1$，$s_i=Q_1\cdots Q_i\ (1\leqslant i\leqslant g)$，则 $W_{s_0}=W_1=\mathbf{Z}[G]$，$W_{s_g}=W$. 在行正合的交换图表$(rQ|\overline{M})$(图2.10)

$$\begin{array}{ccccccccc} 0 & \to & W_r^{T_Q} & \to & W_r & \to & (1-e_Q)W_r & \to & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \to & W_{rQ}^{T_Q} & \to & W_{rQ} & \to & (1-e_Q)W_{rQ} & \to & 0 \end{array}$$

图　2.10

中，我们证明了 $W_r^{T_Q}=W_{rQ}^{T_Q}$，所以$[W_r:W_{rQ}]=1$(注意，这并不表明 $W_r=W_{rQ}$，因为一般来说，W_r 和 W_{rQ}没有包含关系. 我们只是定义

$$[W_r:W_{rQ}]=[W_r+W_{rQ}:W_{rQ}]/[W_r+W_{rQ}:W_r].$$

由此可递归推出

$$[\mathbf{Z}[G]:W]=[W_1:W_M]=1.$$

对每个群同态 $f:A\to B$ 和 A 的子群 A_1和 A_2，熟知有

$$[A_1:A_2]=[f(A_1):f(A_2)][\ker(f)\cap A_1:\ker(f)\cap A_2],$$

于是

$$1=[\mathbf{Z}[G]:W]=[\mathbf{Z}[G]_0:W_0][s(G)\mathbf{Z}[G]:s(G)W]. \tag{2.4.1}$$

但是

$$\begin{aligned} s(G)\mathbf{Z}[G] &= s(G)\mathbf{Z}, \\ s(G)W_Q &= s(G)(s(T_Q)\mathbf{Z}[G]+(1-\bar{\sigma}_Q)\mathbf{Z}[G]) \\ &= s(G)s(T_Q)\mathbf{Z}[G]=\Phi(Q^r)\mathbf{Z}s(G)\quad (Q^r\|M). \end{aligned}$$

因此 $s(G)W=s(G)W_{Q_1}\cdots W_{Q_g}=\Phi(M)\mathbf{Z}s(G)$. 这表明了

$$[s(G)\mathbf{Z}[G]:s(G)W]=\Phi(M).$$

而(2.4.1)式给出了$[\mathbf{Z}[G]_0:W_0]=\Phi(M)^{-1}$. 再考虑同构

$$e^+:\mathbf{Q}[G]\to\mathbf{Q}[G],\quad \alpha\mapsto e^+\alpha\quad \left(e^+=\frac{1}{(q-1)}s(J)\right),$$

又得到(考虑 $\mathbf{Q}[G]$的子群 $\mathbf{Z}[G]_0$和 W_0)

$$\begin{aligned} \Phi(M)^{-1}=[e^+\mathbf{Z}[G]_0:e^+W_0][\ker(e^+) \\ \cap\mathbf{Z}[G]_0:\ker(e^+)\cap W_0]. \end{aligned} \tag{2.4.2}$$

设 σ 是 J 的一个生成元，则

$$
\begin{aligned}
&[\ker(e^+)\cap \mathbf{Z}[G]_0:\ker(e^+)\cap W_0]\\
&\quad=[\ker(e^+)\cap \mathbf{Z}[G]:\ker(e^+)\cap W]\\
&\quad=[(1-\sigma)\mathbf{Z}[G]:(1-\sigma)W][(1-\sigma)W:\ker(e^+)\cap W]\\
&\quad=[(1-\sigma)\mathbf{Z}[G]:(1-\sigma)W]\,|H^1(J,W)|^{-1}\\
&\quad=[(1-\sigma)\mathbf{Z}[G]:(1-\sigma)W](q-1)^{-2^{\kappa-1}}\\
&\qquad(\text{引理 } 2.4.7)\\
&\quad=\prod_{i=1}^{\kappa}[(1-\sigma)W_{r_{i-1}}:(1-\sigma)W_{r_i}](q-1)^{-2^{\kappa-1}}. \qquad (2.4.3)
\end{aligned}
$$

于是问题归结为对于 $rQ|\overline{M}$ 计算$[(1-\sigma)W_r:(1-\sigma)W_{rQ}]$. 由于

$$(1-e_Q)(1-\sigma)W_{rQ}=(1-e_Q)(1-\sigma)W_r,$$

可知

$$
\begin{aligned}
&[(1-\sigma)W_r:(1-\sigma)W_{rQ}]\\
&\qquad=[((1-\sigma)W_r)^{T_Q}:((1-\sigma)W_{rQ})^{T_Q}], \qquad (2.4.4)
\end{aligned}
$$

但是

$$
\begin{aligned}
((1-\sigma)W_{rQ})^{T_Q}&=s(T_Q)(1-\sigma)W_r+(1-\lambda_Q^{-1})((1-\sigma)W_r)^{T_Q}\\
&\subseteq((1-\sigma)W_r)^{T_Q}.
\end{aligned}
$$

记 $B=((1-\sigma)W_r)^{T_Q}/s(T_Q)(1-\sigma)W_r$,则

$$[((1-\sigma)W_r)^{T_Q}:((1-\sigma)W_{rQ})^{T_Q}]=|B/(1-\lambda_Q^{-1})B|. \qquad (2.4.5)$$

由 T_Q-模正合序列$0\to W_r'\to W_r\to(1-\sigma)W_r\to 0$给出正合序列

$$
\begin{aligned}
&H^0(T_Q,W_r)\to H^0(T_Q,(1-\sigma)W_r)\\
&\quad\to H^1(T_Q,W_r')\to H^1(T_Q,W_r).
\end{aligned}
$$

但是 W_r 是自由 T_Q-模,所以

$$
\begin{aligned}
H^0(T_Q,W_r)&=W_r^{T_Q}/s(T_Q)W_r=(0),\\
H^0(T_Q,(1-\sigma)W_r)&=((1-\sigma)W_r)^{T_Q}/s(T_Q)(1-\sigma)W_r=B,\\
H^1(T_Q,W_r)&=(0).
\end{aligned}
$$

于是由上面的正合序列得到

$$B\cong H^1(T_Q,W_r')\cong H^1(J,W_r'^{T_Q}) \quad (\text{引理 } 2.4.5).$$

如果 $rQ\neq\overline{M}$,则 $W_r'^{T_Q}$ 是自由 J-模. 于是 $B=H^1(J,W_r'^{T_Q})=(0)$. 由

(2.4.4)和(2.4.5)式得出

$$[(1-\sigma)W_r:(1-\sigma)W_{rQ}]=1 \quad (rQ\neq \overline{M}).$$

如果 $rQ=\overline{M}$，则 $B\cong H^1(J,W_r^{T_Q})=A_r^+$. 由于 A_r^+ 是平凡 G-模，所以 $(1-\lambda_Q^{-1})B=(0)$. 于是由(2.4.4)和(2.4.5)式给出

$$[(1-\sigma)W_r:(1-\sigma)W_{rQ}]=|A_r^+| \quad (rQ=\overline{M}).$$

综合上述可知

$$\prod_{i=1}^{g}[(1-\sigma)W_{r_{i-1}}:(1-\sigma)W_{r_i}]=[(1-\sigma)W_{r_{g-1}}:(1-\sigma)W_{r_g}]$$

$$=\left|A_{r_{g-1}}^+\right|=\begin{cases}1, & 若\ g=1;\\ (q-1)^{2^g-2}, & 若\ g\geqslant 2.\end{cases}$$

再由(2.4.2)和(2.4.3)式给出

$$[e^+\mathbf{Z}[G]_0:e^+W_0]=\Phi(M)^{-1}(q-1)^{2^{g-1}}\cdot\left|A_{r_{g-1}}^+\right|^{-1}$$

$$=\begin{cases}\Phi(M)^{-1}(q-1), & 若\ g=1;\\ \Phi(M)^{-1}(q-1)^{2^g-2}, & 若\ g\geqslant 2.\end{cases}$$

这就证明了定理2.4.1，从而也最终证明了定理2.3.1. ∎

§2.5　Stickelberg 理想和相对理想类数

设 $k=\mathbf{F}_q(T)$，$K=k(\Lambda_M)$. 定理2.1.1、定理2.2.1和定理2.3.1表明：K^+的理想类数 $h(O_K^+)$可以解释成是 K^+的单位群 U_K^+ 对于它的某种分圆单位子群的指数(乘以一个容易计算的因子). 本节中我们介绍 Shu L[52]对于 K 的相对类数 $h(O_K)^-=h(O_K)/h(O_K^+)$ 给出的一个代数解释，它类似于分圆数域的情形关于 Stickelberger理想的 Iwasawa 和 Sinnott 的结果(见文献[57]定理6.19).

如前一样，我们记($R=\mathbf{F}_q[T]$)：

$$G=\mathrm{Gal}(K/k)=\{\sigma_A:A\in(R/(M))^*\},$$

$$J=\{\sigma_a:a\in\mathbf{F}_q^*\},\quad r=\frac{\Phi(M)}{q-1}-1,$$

$$e^{+}=\frac{1}{q-1}s(J),\quad e^{-}=1-e^{+},$$

$$\mathbf{Z}[G]^{-}=\mathbf{Z}[G]\cap e^{-}\mathbf{Z}[G].$$

引理2.5.1 $[e^{-}\mathbf{Z}[G]:\mathbf{Z}[G]^{-}]=(q-1)^{r+1}$.

证明 我们有加法群同构

$$\frac{\mathbf{Z}[G]+e^{-}\mathbf{Z}[G]}{\mathbf{Z}[G]}\simeq\frac{e^{-}\mathbf{Z}[G]}{\mathbf{Z}[G]^{-}}.$$

于是$[e^{-}\mathbf{Z}[G]:\mathbf{Z}[G]^{-}]=[\mathbf{Z}[G]+e^{-}\mathbf{Z}[G]:\mathbf{Z}[G]]$. 在$e^{-}\mathbf{Z}[G]$中的元素有形式$\alpha=e^{-}\beta$，其中$\beta\in\mathbf{Z}[G]$. 令

$$\beta=\sum_{A\in(R/(M))^{*}}b_{A}\sigma_{A}\quad(b_{A}\in\mathbf{Z}),$$

则

$$\begin{aligned}\alpha&=(1-e^{+})\beta=\beta-\frac{1}{q-1}s(J)\beta\\&=\beta-\frac{1}{q-1}\sum_{A\in(R/(M))^{*}}b_{A}\sigma_{A}\cdot\sum_{a\in\mathbf{F}_q^{*}}\sigma_{a}\\&=\beta-\frac{1}{q-1}\sum_{\substack{A\in R_1\\ \deg A<\deg M}}\sigma_{A}s(J)\sum_{a\in\mathbf{F}_q}b_{aA}.\end{aligned}$$

于是$\alpha\in\mathbf{Z}[G]\Longleftrightarrow\sum_{a\in\mathbf{F}_q^{*}}b_{aA}\equiv0\pmod{q-1}$（对每个$A\in R_1$，$\deg A<\deg M$）. 这就表明$[\mathbf{Z}[G]+e^{-}\mathbf{Z}[G]:\mathbf{Z}[G]]=(q-1)^{r+1}$. ∎

现在我们考虑映射

$$\phi:k/R=\mathbf{F}_q(T)/\mathbf{F}_q[T]\rightarrow\frac{1}{q-1}\mathbf{Z},$$

其中$\phi(0)=0$，而每个k/R中非零元素均可唯一地表示成$\frac{A}{M}$，其中$M\in R_1$，$A\in R$，$\deg A<\deg M$，$(M,A)=1$，我们定义

$$\phi\left(\frac{A}{M}\right)=\begin{cases}\dfrac{q-2}{q-1}，若 A 是首1多项式；\\[2mm]\dfrac{-1}{q-1}，否则.\end{cases}$$

对于$\chi\in\hat{G}$（即χ是模M特征），令F_χ为χ的导子，定义

$$\phi(\chi)=\sum_{A\in(R/(F_\chi))^*}\chi^*(A)\phi\left(\frac{A}{F_\chi}\right).$$

引理2.5.2　(1) 对每个 $M\in R_1$，$\sum_{A\in R/(M)}\phi\left(\frac{A}{M}\right)=0$.

(2) 对每个 $r\in k/R$，$M\in R_1$，

$$\phi(r)=\sum_{\substack{t\in k/R\\ tM=r}}\phi(t)=\sum_{A\in R/(M)}\phi\left(\frac{r+A}{M}\right).$$

(3) 当 χ 为实特征时，$\phi(\chi)=0$. 若 χ 为非实特征，则对每个 $N\in R_1$，$F_\chi|N$，均有

$$\sum_{A\in(R/(N))^*}\chi(N)\phi\left(\frac{A}{N}\right)=\phi(\chi)\prod_{Q|N}(1-\chi^*(Q)),$$

其中右端和式中的 Q 过 N 的所有首1不可约因子.

证明　(1) 当 $M=1$时，由 $\phi(0)=0$知命题成立. 设 $\deg M\geqslant 1$. 则对每个 $A\in R_1$，$\deg A<\deg M$，我们有

$$\sum_{a\in F_q^*}\phi\left(\frac{aA}{M}\right)=\phi\left(\frac{A}{M}\right)+\sum_{1\neq a\in F_q^*}\left(\frac{aA}{M}\right)$$

$$=\frac{q-2}{q-1}-(q-2)\cdot\frac{1}{q-1}=0.$$

由此即知(1) 成立.

(2) 当 $r=0$时，由(1)知(2)中等式两端均为零. 若 $r\neq 0$，则 $r=\frac{C}{D}$，其中 $C\in R$，$D\in R_1$，$(C,D)=1$，并且 $\deg C<\deg D$. 于是

$$\sum_{A\in R/(M)}\phi\left(\frac{r+A}{M}\right)=\sum_{A\in R/(M)}\phi\left(\frac{C+AD}{MD}\right)$$

$$=\phi\left(\frac{C}{MD}\right)+\sum_{0\neq A\in R/(M)}\phi\left(\frac{C+AD}{MD}\right).$$

但是当 $A\neq 0$时，由 $\deg C<\deg D$ 知 $C+AD$ 的最高次项系数即是 A 的最高次数系数. 由此即知上式右端的和式等于零. 于是

$$\sum_{A\in R/(M)}\phi\left(\frac{r+A}{M}\right)=\phi\left(\frac{C}{MD}\right)=\phi\left(\frac{C}{D}\right)=\phi(r).$$

(3) 由(1)的证明可知第一论断成立，第二论断的证明与引理

2.1.3的证明相仿. 以 $Q_1,\cdots,Q_t$ 表示满足 $Q|N$, $Q\nmid F_\chi$ 的所有首1不可约多项式 Q. 并令 $\deg N=d$, $\deg Q_i=d_i$, $\deg F_\chi=d_\chi$. 由于 $F_\chi\Big|\dfrac{N}{Q_1\cdots Q_t}$, 可知 $d_\chi\leqslant d-d_1-d_2-\cdots-d_t$. 我们有

$$\begin{aligned}
\sum_{A\in(R/(N))^*}\chi(N)\phi\left(\frac{A}{N}\right)=&\sum_{A\in(R/(N))^*}\chi^*(N)\phi\left(\frac{A}{N}\right)\\
=&\sum_{\substack{A\in R\\ \deg A<d}}\chi^*\phi\left(\frac{A}{N}\right)\\
&-\sum_{i=1}^{t}\chi^*(Q_i)\sum_{\substack{A\in R\\ \deg A<d-d_i}}\chi^*(A)\phi\left(\frac{AQ_i}{N}\right)\\
&+\sum_{1\leqslant i<j\leqslant t}\chi^*(Q_iQ_j)\\
&\times\sum_{\substack{A\in R\\ \deg A<d-d_i-d_j}}\chi^*(A)\phi\left(\frac{AQ_iQ_j}{N}\right)-\cdots\\
&+(-1)^t\chi^*(Q_1\cdots Q_t)\\
&\times\sum_{\substack{A\in R\\ \deg A<d-d_1-\cdots-d_t}}\chi^*(A)\phi\left(\frac{AQ_1\cdots Q_t}{N}\right).
\end{aligned}\tag{2.5.1}$$

但是对每个 d' 满足 $d_\chi\leqslant d'\leqslant d$, 取 $L\in R_1$ 使 $\deg L=d'$. 则

$$\begin{aligned}
\sum_{\substack{A\in R\\ \deg A<d'}}\chi^*(A)\phi\left(\frac{A}{N}\right)=&\sum_{\substack{A\in R\\ \deg A<d'}}\chi^*(A)\phi\left(\frac{A}{L}\right)\\
=&\sum_{\substack{C\in R\\ \deg C<d_\chi}}\sum_{\substack{B\in R\\ \deg B<d'-d_\chi}}\chi^*(BF_\chi+C)\phi\left(\frac{BF_\chi+C}{L}\right)\\
=&\sum_{C}\chi^*(C)\sum_{\substack{B\in R\\ \deg B<d'-d_\chi}}\phi\left(\frac{B+\frac{C}{F_\chi}}{L/F_\chi}\right)\\
=&\sum_{C}\chi^*(C)\phi\left(\frac{C}{F_\chi}\right)\quad(\text{由}(2))\\
=&\phi(\chi),
\end{aligned}$$

代入(2.5.1)式，可知

$\left(\text{注意 } \phi\left(\frac{AQ_i}{N}\right)=\phi\left(\frac{AQ_iQ_j}{N}\right)=\cdots=\phi\left(\frac{A}{N}\right)\right)$

$$\begin{aligned}\sum_{A\in(R/(N))^*}\chi(N)\phi\left(\frac{A}{N}\right)&=\phi(\chi)\Big[1-\sum_{i=1}^{t}\chi^*(Q_i)\\&\quad+\sum_{1\le i<j\le t}\chi^*(Q_iQ_j)-\cdots\\&\quad+(-1)^t\chi^*(Q_1\cdots Q_t)\Big]\\&=\phi(\chi)\prod_{i=1}^{t}(1-\chi^*(Q_i))\\&=\phi(\chi)\prod_{Q\mid N}(1-\chi^*(Q)).\qquad\blacksquare\end{aligned}$$

现在我们对于$0\neq A\in R/(M)$定义 Stickelberger 元素

$$\eta'(A)=\sum_{B\in(R/(M))^*}\phi\left(\frac{AB}{M}\right)\sigma_B^{-1},$$

记S是$\mathbf{Q}[G]$中由$\{\eta'(A):0\neq A\in R/(M)\}$生成的加法子群. 当$C\in R$，$(C,M)=1$时，易知$\sigma_C(\eta'(A))=\eta'(CA)$. 由此可知$S$是$\mathbf{Z}[G]$-模. 于是$S^-=\mathbf{Z}[G]\cap S$为$\mathbf{Z}[G]$的一个理想，与数域的情形类比，可把$S^-$称作$\mathbf{Z}[G]$的 Stickelberger 理想.

由于

$$\begin{aligned}e^+\eta'(A)&=\frac{1}{q-1}\sum_{a\in F_q^*}\sigma_a\eta'(A)=\frac{1}{q-1}\sum_{a\in F_q^*}\eta'(aA)\\&=\frac{1}{q-1}\sum_{B\in(R/(M))^*}\sigma_B^{-1}\sum_{a\in F_q^*}\phi\left(\frac{aAB}{M}\right)\\&=0\quad(\text{由于第二个和式为零}),\end{aligned}$$

于是　　$e^-\eta'(A)=(1-e^+)\eta'(A)=\eta'(A).$

这表明$e^-S=S$，所以

$$S^-=e^-S^-=e^-\mathbf{Z}[G]\cap S^-\subseteq e^-\mathbf{Z}[G]\cap\mathbf{Z}[G]=\mathbf{Z}[G]^-.$$

本节的主要目的是证明如下定理：

定理2.5.3[52] 设 g 为 M 的首1不可约因子的个数，则 $[\mathbf{Z}[G]^-:S^-]=h(O_K)^-(q-1)^a$，其中当 $g=1$时 $a=0$，而当 $g\geqslant 2$ 时，$a=2^{g-2}+1$.

定理2.5.3的证明和定理2.3.1的证明很相似. 我们仍利用§2.3中定义的 $\mathbf{Z}[G]$-模 W（以及那里的符号 $\bar{\sigma}_Q$ 和 H_F）. 于是

$$[\mathbf{Z}[G]^-:S^-]=[\mathbf{Z}[G]^-:e^-\mathbf{Z}[G]]\cdot[e^-\mathbf{Z}[G]:e^-W]\\ \times[e^-W:S]\cdot[S:S^-]. \qquad (2.5.2)$$

现在我们计算(2.5.2)式右端 4 个指数的值. 我们已有

[Z[G]⁻:e⁻Z[G]] = (q−1)^[illegible]（引理 2.5.1）.

引理2.5.4 $[S:S^-]=q-1$.

证明 由 $\phi\left(\frac{A}{M}\right)$ 的定义可知（令 $\deg M=d$）:

$$\eta'(1)=\sum_{\substack{A\in R_+\\ \deg A<d}}\sigma_A-\frac{1}{q-1}\sum_{A\in(R/(M))^*}\sigma_A.$$

一般地则有

$$\eta'(A)\equiv-\frac{b}{q-1}\sum_{A\in(R/(M))^*}\sigma_A\equiv b\eta'(1)\pmod{\mathbf{Z}[G]}.$$

其中$0\leqslant b\leqslant q-2$. 由于对每个 $a\in\mathbf{Z}$，$a\eta'(1)\in\mathbf{Z}[G]$ 的充分必要条件是 $a\equiv 0\pmod{q-1}$. 这就表明$[S:S^-]=q-1$. ∎

为了计算另外两个指数值，我们需要如下引理：

引理2.5.5 令

$$\omega'=\sum_{\chi\in\hat{G}}\phi(\bar{\chi})e_\chi=\sum_{\chi\in\hat{G}^-}\phi(\bar{\chi})e_\chi$$

（注意，当 χ 为实特征值时，$\phi(\chi)=0$），则 $S=\omega' W$.

证明 这与证明引理2.3.6的(1)相仿，设 $M=AF$，我们只需证明

$$\eta'(A)=\omega' s(H_F)\prod_{Q\mid F}(1-\sigma_Q). \qquad (2.5.3)$$

这又只需对每个 $\chi\in\hat{G}$，χ^* 在此式两端的取值相等. 若 χ 为实特征，则上式两端的 χ^* 值均为零. 以下设 $\chi\in\hat{G}^-$. 如果 $F_\chi\nmid F$，则

$$\chi^*(\eta'(A))=0,\ \chi^*(s(H_F))=0.$$

所以上式两端的 χ^* 值也均为零. 最后设 $F_\chi | F$, 则

$$\chi^*(\text{右}) = |H_F| \chi^*(\omega') \prod_{Q|F} (1 - \bar{\chi}^*(Q))$$

$$= \frac{\Phi(M)}{\Phi(F)} \phi(\bar{\chi}) \prod_{Q|F} (1 - \bar{\chi}^*(Q));$$

$$\chi^*(\text{左}) = \chi^*(\eta'(A)) = \sum_{B\in (R/(M))^*} \phi\left(\frac{AB}{M}\right) \bar{\chi}^*(B)$$

$$= \frac{\Phi(M)}{\Phi(F)} \sum_{B\in (R/(F))^*} \phi\left(\frac{B}{F}\right) \bar{\chi}^*(B)$$

$$= \chi^*(\text{右}) \quad (\text{由引理 } 2.5.2 \text{ 的}(3)).$$

这就证明了引理2.5.5. ▌

引理2.5.6 $[e^- W:S] = h(K)^-$(K 的相对除子类数).

证明 我们知道 $S = e\ S$, 再由引理2.5.5可知

$$[e\ W:S] = [e^- W:\omega' e\ W].$$

进而, 熟知 $\boldsymbol{C}[G]$ 有正交分解

$$\boldsymbol{C}[G] = \bigoplus_{\chi\in\hat{G}} \boldsymbol{C}[G]_\chi,$$

其中 $\boldsymbol{C}[G]_\chi = \boldsymbol{C}[G] e_\chi$. 由于 $1 = \sum_{\chi\in\hat{G}} e_\chi$, $e^+ = \frac{1}{q-1} \sum_{a\in F_q^*} \sigma_a = \sum_{\chi\in\hat{G}} e_\chi$,

从而 $e^- = \sum_{\chi\in\hat{G}} e_\chi$. 于是 $e^- W \subseteq e^- \boldsymbol{C}[G]$, 并且

$$e^- \boldsymbol{C}[G] = \bigoplus_{\chi\in\hat{G}} \boldsymbol{C}[G]_\chi.$$

另一方面, 当 χ 是实特征时, 有

$$e_\chi \omega' = e_\chi \sum_{\lambda\in\hat{G}} \phi(\bar{\lambda}) e_\lambda = \phi(\bar{\chi}) e_\chi = 0 \quad (\text{引理 } 2.5.2 \text{ 的}(3)).$$

这表明 $\omega' \in e^- \boldsymbol{C}[G]$. 于是我们有线性映射

$$f: e^- \boldsymbol{C}[G] \to e\ \ \boldsymbol{C}[G], \quad f(\alpha) = \omega' \alpha.$$

并且由 $W \cong \boldsymbol{Z}^{\Phi(M)}$(引理2.3.6)可知 W 是 $\boldsymbol{C}[G]$ 中的格, 于是 $e\ W$ 是 $e^- \boldsymbol{C}[G]$ 中的格. 由此可知

$$[e\ W:\omega' e\ W] = |\det(f)| = \prod_{\chi\in\hat{G}} \Big|\ |\phi(\bar{\chi})|$$

$$= \prod_{\chi \in \hat{G}} \left| \sum_{A \in (K/(M))^*} \bar{\chi}^*(A) \phi\left(\frac{A}{M}\right) \right|$$

$$= \prod_{\chi \in \hat{G}^-} \left| \sum_{\substack{A \in K_1 \\ \deg A < \deg M}} \bar{\chi}^*(A) \right|$$

$$= h(K)^- \quad (\text{定理 } 1.5.2). \qquad \blacksquare$$

引理2.5.7 $[e^- - \mathbf{Z}[G] : e^- W] = (q-1)^b$,

其中当 $g=1$时，$b=0$，当 $g \geqslant 2$时，$b=2^{g-2}$.

证明 考虑线性映射

$$f^- : Q[G] \to Q[G],\ f^-(\alpha) = e^- \alpha.$$

则对于$Q[G]$的两个子群 $\mathbf{Z}[G]$和 W，有

$$\begin{aligned}[\mathbf{Z}[G] : W] &= [e^- \mathbf{Z}[G] : e^- W] \\ &\quad \times [\ker(f^-) \cap \mathbf{Z}[G] : \ker(f^-) \cap W] \\ &= [e^- \mathbf{Z}[G] : e^- W] \cdot [\mathbf{Z}[G]' : W'].\end{aligned}$$

在定理2.4.1的证明中，我们曾得到$[\mathbf{Z}[G] : W] = 1$. 于是

$$[e^- \mathbf{Z}[G] : e^- W] = [W' : \mathbf{Z}[G]'].$$

但是

$$H^0(J, W) = \frac{W'}{s(J)W},\ \mathbf{Z}[G]' = s(J)\mathbf{Z}[G],$$

于是

$$\begin{aligned}[W' : \mathbf{Z}[G]'] &= |H^0(J, W)| \cdot [s(J)W : s(J)\mathbf{Z}[G]] \\ &= |H^0(J, W)| \cdot [e^+ W : e^+ \mathbf{Z}[G]].\end{aligned}$$

再考虑映射

$$f^+ : Q[G] \to Q[G], f^+(\alpha) = e^+ \alpha,$$

又得到

$$\begin{aligned}[e^+ W : e^+ \mathbf{Z}[G]] &= [\ker(f^+) \cap \mathbf{Z}[G] : \ker(f^+) \cap W] \\ &= \begin{cases} (q-1)^{-1}, & \text{若 } g = 1; \\ (q-1)^{-2^{g-2}}, & \text{若 } g \geqslant 2. \end{cases} \quad (\text{见 §2.4 末尾})\end{aligned}$$

由引理2.4.7算出了$|H^0(J, W)| = (q-1)^{2^{g-1}}$. 最后得到

$$[e^- \mathbf{Z}[G] : e^- W] = |H^0(J, W)| \cdot [e^+ W : e^+ \mathbf{Z}[G]]$$

$$= \begin{cases} 1, 若\ g = 1; \\ (q-1)^{2^g \ 2}, 若\ g \geqslant 2. \end{cases}$$ ▌

至此，我们将(2.5.2)式右端的4个因子均已算出了. 于是

$$[\mathbf{Z}[G] \ ; S \ ] = (q-1)^{r \ 1}(q-1)h(K) \ (q-1)^{r}$$
$$= h(K) \ (q-1)^{r \ r}.$$

再由系1.5.3可知当 $g=1$ 时，

$$[\mathbf{Z}[G] \ ; S \ ] = h(K) \ (q-1)^{r} = h(O_K) \ ;$$

而当 $g \geqslant 2$ 时，

$$[\mathbf{Z}[G] \ ; S \ ] = h(K) \ (q-1)^{r \ r} = h(O_K) \ (q-1)^{r \ 1}$$
$$= h(O_K)(q-1)^{2^g \ 2 \ r}.$$

这就完成了定理2.5.3的证明. ▌

第 3 章

欧 拉 系

在前一章里我们已经看到,分圆单位群在整个单位群中的指数与分圆域的极大实子域的类数有密切关系.事实上,它们之间有更深一层的联系.在分圆数域的情形,Gras[32]在 70 年代末曾提出如下的猜想:若 p 是奇素数,并且 p 与分圆域 $K=\boldsymbol{Q}(\zeta_m)$的扩张次数互素(即$(p,\varphi(m))=1$),则理想类群 C_K 的 p 部分和商群 $U_K/C_y(K)$ ($C_y(K)$为 K 的分圆单位群)的 p 部分作为伽罗华模有相同的 Jordan-Hölder 序列.此后不久,Greenberg[34]指出了分圆域的主猜想可以推出上述 Gras 猜想(关于分圆域主猜想的内容可参看文献[57]).到了 80 年代,Mazur 和 Wiles[47]证明了分圆域的主猜想.但是其证明方法采用了艰深的代数几何,而且证明过程很长.80 年代末,Thaine[53]提出了利用分圆单位研究理想类群的一个"新"想法,事实上,这个想法早在一百多年前就隐含在 Kummer[44]的文章中了,可惜一直被人们所忽视.最近,Kolyvagin[43]提出了欧拉系的概念,使 Thaine 的想法可以递推地进行下去.作为欧拉系的一个具体应用,他给出了 Gras 猜想的一个简单而直接的证明,并且他认为分圆域的主猜想也可用这种方法直接证明.Rubin[50]发展了 Kolyvagin 的工作,给出了分圆域的主猜想一个简单而初等的证明.

本章的目的是利用欧拉系的方法证明 Gras 猜想在函数域上的模拟.确切地说,对于分圆函数域 $K=k(\Lambda_M)$ ($k=\boldsymbol{F}_q(T)$),记 $F=K^+$ (极大实子域),$G=\mathrm{Gal}(F/k)$,取定一个素数 l,满足

$(l, q\Phi(M))=1$. 若 Δ 是域 F 的理想类群的 l-sylow 子群. 根据定理 2.3.1, $|\Delta|$ 等于 U/C 的 l-sylow 子群的阶. 注意, Δ 和 U/C 都可看成是 $\mathbf{Z}_l[G]$-模. 我们要证明的是: 对于 G 的每个不可约的 $\mathbf{Z}_l$ 表示 χ, 这两个 $\mathbf{Z}_l[G]$-模的 χ 分支有相同的阶(定理 3.3.3).

本章的安排如下: §3.1 首先引入欧拉系的概念, 由分圆单位构造出欧拉系, 可以得出域 F 中一批元素的素理想分解式, 这就给出域 F 的理想类群的一批关系, 而且这些关系与分圆单位有密切联系. 在 §3.2 节, 我们从这批关系中挑选出有用的"好"关系, 主要工具是 Chebotarev 定理. 在 §3.3 节中, 利用挑选出来的关系证明上面提到的结论.

除了前面已经给出的标准符号之外, 再引入以下一些记号:

N: 素数 l 的某个方幂

$$S_N=\left\{\prod_{i=1}^{n}Q_i: Q_i \text{ 是 } R \text{ 中两两不同的首 1 不可约多项式,}\right.$$
$$\left.\text{在 } F \text{ 中均完全分裂, 并且 } N\mid\Phi(Q_i)\ (1\leqslant i\leqslant n)\right\}$$

对于每个 $J\in S_N$, 令

$$G_J=\mathrm{Gal}(F(\Lambda_J)/F)=\mathrm{Gal}(k(\Lambda_J)/k)$$

$$N_J=\sum_{\tau\in G_J}\tau\in\mathbf{Z}[G_J]\ \text{(Norm 算子)}$$

若 Q 是 S_N 中一个首 1 不可约多项式, 令

σ_Q 为 G_Q 的一个固定的生成元

$$D_Q=\sum_{i=1}^{\Phi(Q)-1} i\sigma_Q^i\in\mathbf{Z}[G_Q]$$

对于每个 $J\in S_N$, 令

$$D_J=\prod_{Q\mid J}D_Q\in\mathbf{Z}[G_J]$$

I: F 的分式理想群

I_Q: F 中 Q 的素理想因子生成的 I 的子群

对于 $y\in F^*$, 令

$[y]$: 主理想 $(y)=yO_F$ 在商群 I/NI 中的投影(这里 I 中运算

采用加法，NI 是 I 中所有元素的 N 倍构成的子群）

$[y]_Q$：主理想(y)在商群 I_Q/NI_Q 中的投影

设 A 是 R 中首 1 多项式，令

λ_A 为循环 R-模 Λ_A 的一个固定的生成元

§3.1 欧 拉 系

我们的目的是想构作出域 F 中的一系列元素，这些元素有比较容易"控制"的素理想分解，并且这些元素自然与分圆单位有关．所以我们从 F 的一系列阿贝尔扩张中的分圆单位着手论述．

令 C^+是§2.3节中定义的 $K=k(\Lambda_M)$的分圆单位群，则 C^+中元素可表为

$$\eta = a\prod_i \lambda_i / \prod_j \lambda'_j \quad (\lambda_i, \lambda'_j \in \Lambda_M, a \in F_q^*). \qquad (3.1.1)$$

对于 $J\in S_N$，定义

$$\xi_J(\eta)= \Big(\prod_i N_{k(\Lambda_{MJ})/F(\Lambda_J)}(\lambda_i - \sum_{P|J}\lambda_P)\Big) \Big/ \Big(\prod_j N_{k(\Lambda_{MJ})/F(\Lambda_J)}(\lambda'_j - \sum_{P|J}\lambda_P)\Big)$$

这里 P 过 J 的首 1 不可约因子．

可以验证元素 $\xi_J(\eta)(\eta\in C^+, J\in S_N)$满足如下三条性质：

(1) $\xi_J(\eta)$是 $F(\Lambda_J)$中的单位；

(2) $N_Q(\xi_J(\eta))=(Fr_Q-1)\xi_{J/Q}(\eta)$，

式中 Q 是 J 的首 1 不可约因子，而 Fr_Q 是 Q 在 $G_{J/Q}$中的 Frobenius 自同构元素；

(3) $\xi_J(\eta)\equiv\xi_{J/Q}(\eta) \pmod{\mathscr{P}}$，

其中 $\mathscr{P}$ 是 Q 在 $F(\Lambda_J)$中的任意素理想因子．

证明 性质(3)可由定理 1.2.1 直接推出．现在证明性质(2)：记 $J_1=J/Q\in R$，由于 $\lambda-\sum_{P|J_1}\lambda_P\in\Lambda_{MJ_1}$，并且

$$\mathrm{Gal}(k(\Lambda_{MJ})/k(\Lambda_{MJ_1}))\cong \mathrm{Gal}(k(\Lambda_Q)/k),$$

所以

$$N_Q\Big(N_{k(\Lambda_{MJ})/F(\Lambda_J)}(\lambda-\sum_{P|J}\lambda_P)\Big)$$

$$=N_{k(\Lambda_{MJ_1})/F(\Lambda_{J_1})}\left(\frac{\lambda^Q-\sum_{P|J_1}\lambda_P^Q}{\lambda-\sum_{P|J_1}\lambda_P}\right)$$

$$=N_{k(\Lambda_{MJ_1})/F(\Lambda_{J_1})}\Big((Fr_Q^{-1})(\lambda-\sum_{P|J_1}\lambda_P)\Big).$$

由此即得性质(2). 利用性质(2)，对 J 的不可约因子的个数应用归纳法，即可证明性质(1). ▌

由 $\xi_J(\eta)$的定义可以看出，它不仅依赖于 η，还依赖于 η 的表达式(3.1.1). 如果 η 可以表示成

$$\eta=\prod_i\lambda_i^{q-1}/\prod_j\lambda_j'^{q-1}\quad(\lambda_i,\lambda_j'\in\Lambda_M),$$

则 $\xi_1(\eta)=\eta^{q-1}$. 我们称$\{\xi_J(\eta)\}_J$ 是从 η 开始的欧拉系. 欧拉系中的元素均属于 F 的某个阿贝尔扩域. 下面用它们可得出 F 中的元素.

引理 3.1.1　对于 $J\in S_N$，则

$$D_J(\xi_J(\eta))\in\big[F(\Lambda_J)^*/(F(\Lambda_J)^*)^N\big]^{G_J}.$$

对于式中群 G 和 G-模 A，我们记

$$A^G=\{\alpha\in A:g(\alpha)=\alpha\quad(\text{对每个 }g\in G)\}.$$

证明　设 Q 为 J 的首 1 不可约因子，$J=J_1Q$，则易验证有

$$(\sigma_Q-1)D_J=(\Phi(Q)-N_Q)D_{J_1}.$$

根据性质(2)可知

$$(\sigma_Q-1)D_J(\xi_J(\eta))=(\Phi(Q)-N_Q)D_{J_1}(\xi_J(\eta))$$

$$\equiv(1-Fr_Q)D_{J_1}(\xi_{J_1}(\eta))$$

$$\big(\mathrm{mod}(F(\Lambda_J)^*)^{\Phi(Q)}\big).$$

由于 $Fr_Q\in G_{J_1}$，再用归纳法即可证明引理 3.1.1． ▌

引理 3.1.1 表明了 $D_J(\xi_J(\eta))$在 $\mathrm{mod}(F(\Lambda_J)^*)^N$ 的意义下是在伽罗华群 $G_J=\mathrm{Gal}(F(\Lambda_J)/F)$作用下不变的元素. 由伽罗华理

论的启发，它在某种意义下应当对应于 F 中的元素(引理 3.1.2). 为证此结论，我们需要如下著名的定理：

Hilbert 定理 90 设 E/F 是域的有限伽罗华扩张，$G=\mathrm{Gal}(E/F)$. 则 $H^1(G,E^*)$是平凡的.

证明 设 $E=F(\theta)$(有限伽罗华扩张必是单扩张)，$[E:F]=n$. 按照定义，$H^1(G,E^*)$是平凡的，当且仅当 $A=B$，其中

$A=\{f:G\to E^* \mid$ 对任意 $\sigma,\tau\in G, f(\sigma\tau)=(\sigma f(\tau))\}$,

$B=\{f:G\to E^* \mid$ 存在 $\alpha\in E^*$，使得对每个 $\sigma\in G, f(\sigma)=\sigma(\alpha)/\alpha\}$.

显然 $B\subseteq A$. 现在设 $f\in A$. 当 $\tau,\sigma\in G,\tau\neq\sigma$ 时，$\tau(\theta)\neq\sigma(\theta)$. 由此易知存在 i_0 $(0\leqslant i_0\leqslant n-1)$，使得

$$\sum_{\sigma\in G}f(\sigma)\sigma(\theta^{i_0})\neq 0$$

(否则，便有 $f(\sigma)=0$ $(\forall\ \sigma\in G)$，这与 $f(\sigma)\in E^*$ 相矛盾). 现在记 $\beta=\sum_{\tau\in G}f(\tau)\tau(\theta^{i_0})\in E^*$，则对每个 $\sigma\in G$，有

$$\begin{aligned}\sigma\beta &= \sum_{\tau\in G}(\sigma f(\tau))(\sigma\tau(\theta^{i_0})) = \sum_{\tau\in G}f(\sigma)^{-1}f(\sigma\tau)(\sigma\tau(\theta^{i_0}))\\ &= f(\sigma)^{-1}\beta.\end{aligned}$$

于是 $f(\sigma)=\sigma(\beta^{-1})/\beta^{-1}$，即 $f\in B$. 这就证明了 Hilbert 定理 90. ▌

现在将 Hilbert 定理 90 用于引理 3.1.1.

引理 3.1.2 对于 $J\in S_N$，存在 $K_J\in F^*/(F^*)^N$，满足

$$K_J\equiv D_J(\xi_J(\eta))\quad(\mathrm{mod}(F(\Lambda_J)^*)^N).$$

证明 由假设$(N,(q-1)\Phi(M))=1$ 可知 $F(\Lambda_J)$中 N 次单位根只有 1. 根据引理 3.1.1，对每个 $\sigma\in\mathrm{Gal}(F(\Lambda_J)/F)$，存在唯一的 $f_\sigma\in F(\Lambda_J)^*$，满足

$$\sigma D_J(\xi_J(\eta))=f_\sigma^N D_J(\xi_J(\eta)),$$

并且对 $\tau\in\mathrm{Gal}(F(\Lambda_J)/F)$，则

$$\begin{aligned}f_{\tau\sigma}^N D_J(\xi_J(\eta))) &= \tau\sigma(D_J(\xi_J(\eta)) = \tau(f_\sigma^N D_J\xi_J(\eta))\\ &= (\tau f_\sigma)^N\tau(D_J\xi_J(\eta)) = (\tau f_\sigma)^N f_\tau^N\cdot(D_J\xi_J(\eta)).\end{aligned}$$

这表明 $f_{\tau\sigma}=(\tau f_\sigma)\cdot f_\tau$. 由 Hilbert 定理 90 知，存在 $\beta\in F(\Lambda_J)^*$，

使得对每个 $\sigma\in \mathrm{Gal}(F(\Lambda_J)/F)$，$f_\sigma=(\sigma-1)\beta$，即有

$$\sigma(D_J\xi_J(\eta)/\beta^N)=D_J\xi_J(\eta)/\beta^N.$$

这表明 $D_J\xi_J(\eta)/\beta^N\in F$. 取此元素为 K_J. 即得证明. ∎

现在我们要研究 F 中的元素 K_J 的素理想分解的信息. 确切地说，我们想决定 F 中的主理想 $(K_J)=K_JO_F$ 在 I_Q/NI_Q 中的投影 $[K_J]_Q$，其中 Q 是 S_N 中的任意首 1 不可约多项式(命题 3.1.5). 作为准备，我们先证明一个引理，这个引理是说：对于 F 中的每个理想类 a 都存在不可约多项式 $Q\in S_N$，使得类 a 中有素理想 $\mathscr{P}$ 作为代表元，并且 $\mathscr{P}|Q$. 进而对每个不可约多项式 $Q\in S_N$ 和每个 $\alpha\in F^*$，一定存在 $\beta\in F(\Lambda_Q)$，使得 F 中的主理想 (α) 和 $(N_Q(\beta))$ 在 I_Q 中的投影相等. 最后，对每个 $\alpha\in F^*$，$[\alpha]_Q$ 可由 $(O_F/QO_F)^*$ 中一个相应的元素给出.

$$\begin{array}{ccc} & F(\Lambda_Q)^* & \\ {\scriptstyle x\mapsto(1-\sigma_Q)x}\swarrow & & \searrow{\scriptstyle x\mapsto[N_Q(x)]_Q} \\ (O_F/Q\,O_F)^* & \xrightarrow[\varphi_Q]{} & I_Q/NI_Q \end{array}$$

图　3.1

引理 3.1.3　对每个首 1 不可约多项式 $Q\in S_N$，存在唯一的 G-模满同态：

$$\varphi_Q:(O_F/QO_F)^*\to I_Q/NI_Q,$$

使得上面的图表(图 3.1)是交换的.

证明　由于 σ_Q 是

$$\mathrm{Gal}(F(\Lambda_Q)/F)\cong \mathrm{Gal}(k(\Lambda_Q)/k)\cong (R/(Q))^*$$

的生成元，所以 $\sigma_Q(\lambda_Q)=\lambda_Q^A$，其中 A 是 $(R/(Q))^*$ 的生成元. 由于

$$(\sigma_Q-1)\lambda_Q=\lambda_Q^A/\lambda_Q\equiv A \pmod{\lambda_Q},$$

这表明 $(1-\sigma_Q)\lambda_Q$ 是 $(R/(Q))^*$ 的生成元. 又由于 Q 在 F 中分裂为：

$$QO_F=\mathscr{P}_1\cdots\mathscr{P}_g,$$

$$O_F/\mathscr{P}_i\cong R/(Q)\quad(1\leqslant i\leqslant g),$$

$$g=[F:k]=\Phi(M)/(q-1),$$

而每个 $\mathscr{P}_i$ 在 $F(\Lambda_Q)$ 中完全分歧为：

$$\mathscr{P}_i = \mathfrak{P}_i^{\Phi(Q)} \quad (1 \leqslant i \leqslant g).$$

根据中国剩余定理,对每个 i $(1\leqslant i\leqslant g)$有 $y_i\in F(\Lambda_Q)$,满足

$$y_i \equiv \begin{cases} 1 \pmod{\mathfrak{P}_j} \\ \lambda_Q \pmod{\mathfrak{P}_i^2} \end{cases} (\text{对于 } j\neq i, 1\leqslant j\leqslant g),$$

这时

$$(1-\sigma_Q)y_i \equiv \begin{cases} 1 \pmod{\mathfrak{P}_j} \\ (1-\sigma_Q)\lambda_Q \pmod{\mathfrak{P}_i} \end{cases} (\text{对于 } j\neq i).$$

这表明图 3.1 中左侧的映射是满射的. 这个映射的核中元素 $\alpha\in F(\Lambda_Q)^*$ 是满足条件

$$v_{\mathfrak{P}_i}(\alpha) \equiv 0 \pmod{\Phi(Q)} \quad (1\leqslant i\leqslant g)$$

的那些 α. 图3.1中右侧的映射显然是满射的. 并且其核包含左侧映射的核. 由此得到映射 φ_Q,并且可直接看出 φ_Q 是 G-模同态. ▌

注记 3.1.4 根据上面的证明,可以把 φ_Q 明确地表达出来,令 $\epsilon_i=(1-\sigma_Q)y_i$ 是$(O_F/\mathscr{P}_i)^*$的生成元,$y_i\in F(\Lambda_Q)$ $(1\leqslant i\leqslant g)$,则元素

$$x \in (O_F/QO_F)^* \cong \prod_{i=1}^{g}(O_F/\mathscr{P}_i)^*$$

可以表示成 $x=\prod_{i=1}^{g}\epsilon_i^{a_i}$,于是

$$\varphi_Q(x) = \prod_{i=1}^{g}\mathscr{P}_i^{a_i} \in I_Q/NI_Q.$$

所以

$$x \in \operatorname{Ker}\varphi_Q \Leftrightarrow N\,|\,a_i \quad (1\leqslant i\leqslant g) \Leftrightarrow x^{\frac{\Phi(Q)}{N}} = 1.$$

也就是说:

$$\operatorname{Ker}\varphi_Q = \left\{a \in (O_F/QO_F)^* : a^{\frac{\Phi(Q)}{N}} = 1\right\}.$$

由此可知 φ_Q 可以看成是 G-模满同态:

$$\varphi_Q:\{y \in F^*/(F^*)^N : [y]_Q = 0\} \to I_Q/NI_Q.$$

现在给出$[K_J]_Q\in I_Q/NI_Q$ 的一个递推公式如下:

命题3.1.5 设 $J\in S_N$,Q 是 R 中首 1 不可约多项式. 则

$$[K_J]_Q = \begin{cases} 0, 若 Q \nmid J; \\ \varphi_Q(K_{J/Q}), 若 Q \mid J. \end{cases}$$

证明 根据引理3.1.2可知道有 $\beta_J \in F(\Lambda_J)^*$，使得 $K_J = D_J(\xi_J(\eta))/\beta_J^N$. 如果 $Q \nmid J$，则 F 中的每个素理想 $\mathscr{P} \mid Q$ 在 $F(\Lambda_J)$ 中均不分歧. 再由性质(1)知 $D_J(\xi_J(\eta))$ 为单位，于是$[K_J]_Q = 0$. 以下设 $Q \mid J$，记 $J = J_1 Q$，则存在 $\beta_{J_1} \in F(\Lambda_{J_1})^*$，使得 $K_{J_1} = D_{J_1}(\xi_{J_1}(\eta))/\beta_{J_1}^N$，并且由前述，我们可选取 β_{J_1} 在 Q 处是单位. 于是

$$\begin{aligned}(1-\sigma_Q)\beta_J^N &= (1-\sigma_Q)D_J(\xi_J(\eta)) = (N_Q - \Phi(Q))D_{J_1}(\xi_{J_1}(\eta)) \\ &= D_{J_1}N_Q\xi_J(\eta)/(D_{J_1}\xi_J(\eta))^{\Phi(Q)} \\ &= (Fr_Q - 1)D_{J_1}(\xi_{J_1}(\eta))/(D_{J_1}\xi_J(\eta))^{\Phi(Q)} \\ &= (Fr_Q - 1)\beta_{J_1}^N/(D_{J_1}\xi_J(\eta))^{\Phi(Q)}.\end{aligned}$$

因此

$$(1-\sigma_Q)\beta_J = (Fr_Q - 1)\beta_{J_1}/(D_{J_1}\xi_J(\eta))^{\frac{\Phi(Q)}{N}},$$

对于 $F(\Lambda_J)$的每个素理想 $\mathfrak{P} \mid Q$，有

$$\begin{aligned}(1-\sigma_Q)\beta_J &\equiv \beta_{J_1}^{\Phi(Q)}/(D_{J_1}\xi_{J_1}(\eta))^{\frac{\Phi(Q)}{N}} \\ &\equiv \left(K_{J_1}^{-1}\right)^{\frac{\Phi(Q)}{N}} \pmod{\mathfrak{P}}.\end{aligned}$$

由于 $D_J(\xi_J(\eta))$ 为单位，Q 在$F(\Lambda_Q)/F$中完全分歧，所以有 $\gamma \in F(\Lambda_Q)$使得 $\beta_J \cdot \gamma^{\frac{\Phi(Q)}{N}}$ 在 $F(\Lambda_Q)$的每个素理想 $\mathfrak{P} \mid Q$ 之处均是单位. 于是$[N_Q\gamma]_Q = [K_J]_Q$，并且

$$(1-\sigma_Q)\gamma^{\frac{\Phi(Q)}{N}} \equiv (1-\sigma_Q)\beta_J^{-1} \equiv \left(K_{J_1}\right)^{\frac{\Phi(Q)}{N}} \pmod{\mathfrak{P}}.$$

再由引理3.1.3和注记3.1.4即可证明命题3.1.5. ∎

§ 3.2 Chebotarev 定理及其应用

我们已经从 F 的任一个分圆单位出发得出 F 中的一系列元素 $\{K_J : J \in S_N\}$. 在这一节的工作是挑选出所需要的 J. 需用的工

具是 Chebotarev 定理，这是关于算术级数中素数密度的 Dirichlet 定理在整体域中的推广.

Chebotarev 定理 设 E/K 是整体域的伽罗华扩张，$\sigma\in \mathrm{Gal}(E/K)$. 则 K 中存在无限多个次数为1的素理想，使得它们所对应的 Frobenius 自同构均属于 σ 在群 G 中的共轭类.

证明 见文献[57]中§12，定理12. ▌

注记3.2.1 更精确的结果为以 $\tilde{\sigma}$ 表示 σ 在 G 中的共轭类，则上述素理想的密度为 $\frac{|\tilde{\sigma}|}{|G|}=\frac{|\tilde{\sigma}|}{[E:K]}$.

以下我们用 Δ 表示 F 的理想类群的 l-sylow 部分.

定理3.2.2 设 $\hat{u}\in\Delta$，W 是 $F^*/(F^*)^N$ 的有限 G-子模，ψ 是从 W 到 $(\mathbf{Z}/N\mathbf{Z})[G]$ 的 G-模同态. 则 F 中有无限多个素理想 $\mathscr{P}$ 满足以下三个条件：

(1) $\mathscr{P}$ 的理想类为 $\hat{u}$；

(2) $\mathscr{P}|Q$，其中 Q 为 S_N 中首 1 不可约多项式；

(3) 对每个 $w\in W$，均有 $[w]_Q=0$，并且存在 $u\in(\mathbf{Z}/N\mathbf{Z})^*$，使得对每个 $w\in W$，均有 $\varphi_Q(w)=u\psi(w)\mathscr{P}$.

证明 设 H 是 F 的 Hilbert l-类域，即指 H 是 F 的最大不分歧阿贝尔 l-扩张，并且 F 的所有无限素除子在 H 中均完全分裂. 由 Rosen[49]的结果知：Δ 同构于 $\mathrm{Gal}(H/F)$，并且同构为 Artin 映射. 由假设条件

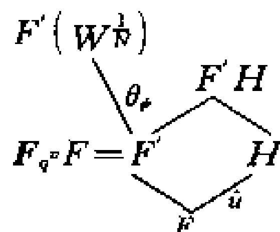


图 3.2

$$(N,q)=(l,q)=1,$$

于是有 v 使 $N|q^v-1$. 令 $F'=F\boldsymbol{F}_{q^v}$(常数域扩张)，由于 F 的无限素除子在 F'中是惰性的，可知 $F'\cap H=F$. 事实上，我们有 $F'(W^{\frac{1}{N}})\cap H=F$(见图3.2). 这是由于

$$\mathrm{Gal}(F'/F)\cong\mathrm{Gal}(\boldsymbol{F}_{q^v}/\boldsymbol{F}_q)$$

为 v 阶循环群. 令 τ 为此群的 Frobenius 生成元，我们考虑 τ 在 $\mathrm{Gal}(F'(W^{\frac{1}{N}})/F')$ 上的作用，设 $\sigma\in\mathrm{Gal}(F'(W^{\frac{1}{N}})/F')$，对每个 $w\in W^{\frac{1}{N}}$，记 $\tilde{\tau}$ 是 τ 到 $F'(W^{\frac{1}{N}})$ 上的一个提升，则

$$\tilde{\tau}(w^{\frac{1}{N}}) = \zeta w^{\frac{1}{N}}, \quad \sigma(w^{\frac{1}{N}}) = \eta w^{\frac{1}{N}},$$

其中 ζ、$\eta \in \boldsymbol{F}_{q^v}^*$. 于是有

$$\tilde{\tau}\sigma\tilde{\tau}^{-1}(w^{\frac{1}{N}}) = \tilde{\tau}\sigma(\tilde{\tau}^{-1}(\zeta^{-1})w^{\frac{1}{N}}) = \tilde{\tau}(\tilde{\tau}^{-1}(\zeta^{-1})\sigma(w^{\frac{1}{N}}))$$

$$= \zeta^{-1}\tilde{\tau}(\eta w^{\frac{1}{N}}) = \zeta^{-1}\eta^{q}\zeta w^{\frac{1}{N}} = \eta^{q} w^{\frac{1}{N}} = \sigma^{q}(w^{\frac{1}{N}}).$$

这表明 $\tilde{\tau}\sigma\tilde{\tau}^{-1} = \sigma^{q}$. 另一方面, $F'H$ 是 F' 的阿贝尔扩张, 从而 τ 在 $\mathrm{Gal}(F'H/F')$ 上的作用是平凡的. 再注意到 $F'(W^{\frac{1}{N}})/F'$ 是 Kummer 扩张, $\mathrm{Gal}(F'(W^{\frac{1}{N}})/F')$ 中元素的阶均为 N 的因子. 但是 $(N,(q-1)) \mid (N,\Phi(M))=1$, 故必有 $F'(W^{\frac{1}{N}}) \cap F'H = F'$. 于是

$$F'(W^{\frac{1}{N}}) \cap H = F' \cap H = F.$$

接下来证明 $F^*/(F^*)^N$ 可自然地视为 $(F')^*/(F'^*)^N$ 的子群. 即要证明

$$F^* \cap (F'^*)^N = (F^*)^N.$$

设 $a \in F^*$, $a = b^N$, $b \in (F')^*$. 取 ε 为循环乘法群 $\boldsymbol{F}_{q^v}^*$ 的生成元, 则有整数 m, 使得 $\tau b = \varepsilon^m b$. 由于 $b = \tau^N b = \varepsilon^{mN} b$, 所以 $\varepsilon^{mN} = 1$, 于是 $(q^v - 1) \mid mN$. 但是 $(N, q-1) = 1$, 因此 $(q-1) \mid m$. 令 $c = \varepsilon^{-\frac{m}{q-1}} b$, 则有

$$\tau(c) = \varepsilon^{\frac{-mq}{q-1}} \tau(b) = \varepsilon^{\frac{-mq}{q-1}} \varepsilon^m b = c,$$

即 $c \in F^*$. 于是

$$a = b^N = c^N \cdot \varepsilon^{\frac{m}{q-1}N} \in (F^*)^N.$$

根据 Kummer 扩张理论, 我们有

$$\mathrm{Gal}(F'(W^{\frac{1}{N}})/F') \cong \mathrm{Hom}(W, \boldsymbol{F}_{q^v}^*).$$

定义群同态 $\theta: (\boldsymbol{Z}/N\boldsymbol{Z})[G] \to \boldsymbol{F}_{q^v}^*$ 满足: 对于 $g \in G$, 有

$$\theta(g) = \begin{cases} \zeta_N, & \text{若 } g = 1_G; \\ 1, & \text{否则}. \end{cases}$$

其中 ζ_N 是 $\boldsymbol{F}_{q^v}^*$ 中一个固定的 N 次本原单位根. 于是 $\theta\Psi \in \mathrm{Hom}(W, \boldsymbol{F}_{q^v}^*)$. 根据 Kummer 对应, 存在 $\gamma \in \mathrm{Gal}(F'(W^{\frac{1}{N}})/F')$, 使得对所有 $w \in W$, 有

$$\theta\psi(w) = \gamma(w^{\frac{1}{N}})/w^{\frac{1}{N}}.$$

$HF'(W^{\frac{1}{N}})/F$ 是伽罗华扩张，并且存在 $\alpha\in\mathrm{Gal}(HF'(W^{\frac{1}{N}})/F)$，使得

$$\alpha|_H=\hat{u},\quad \alpha|_{F(W^{\frac{1}{N}})}=\gamma.$$

由 Chebotarev 定理，F 中存在无限多次数为 1 的素理想 $\mathscr{P}$，其对应的 Frobenuis 自同构属于 α 的共轭类. 我们在下面证明这些素理想满足定理3.2.2的三个条件.

1）由 Artin 映射和 $\alpha|_H=\hat{u}$ 即知满足条件(1)；

2）由于 α 在 F' 上为恒等自同构，而 $Q=\mathscr{P}\cap R$ 在 F' 中完全分裂，所以 $q^v-1|\Phi(Q)$，即 $Q\in S_N$，也即满足条件(2)；

3）$\mathscr{P}$ 在 $F(W^{\frac{1}{N}})/F$ 中不分歧，所以对每个 $w\in W$，有$[w]_Q=0$，于是 w 可自然地看成$(O_F/QO_F)^*$中的元素. 对于由注记3.1.4给出的$(O_F/\mathscr{P})^*$的生成元 ϵ，则有 $w\equiv\epsilon^{a(w)}\pmod{\mathscr{P}}$. 定义群同态：

$$\mathrm{Log}_{\mathscr{P}}\varphi_Q: W\to \mathbf{Z}/N\mathbf{Z},\quad w\mapsto a(w).$$

由于 $N|\Phi(Q)$，这个同态是可定义的. 记 Pr 为 $\mathbf{Z}/N\mathbf{Z}[G]$到 $\mathbf{Z}/N\mathbf{Z}$ 在1_G 分量上的投射，则又有群同态：

$$Pr\cdot\psi: W\to\mathbf{Z}/N\mathbf{Z},$$

并且

$$\begin{aligned}
x\in \mathrm{Ker}(Pr\circ\psi) &\Longleftrightarrow \theta\psi(x)=1\Longleftrightarrow \gamma(x^{\frac{1}{N}})=x^{\frac{1}{N}}\\
&\Longleftrightarrow \tau\mathrm{Frob}(\mathscr{P})\tau^{-1}(x^{\frac{1}{N}})=x^{\frac{1}{N}}\\
&\qquad (\text{对每个 } \tau\in\mathrm{Gal}(HF'(W^{\frac{1}{N}})/F))\\
&\Longleftrightarrow \tau^{-1}(x^{\frac{1}{N}})\in(O_F/\mathscr{P})^*\Longleftrightarrow x\in(O_F/\mathscr{P})^{*N}\\
&\Longleftrightarrow x\in\mathrm{Ker}(\mathrm{Log}_{\mathscr{P}}\varphi_Q).
\end{aligned}$$

注意到 $\mathbf{Z}/N\mathbf{Z}$ 是循环群，所以有 $u\in(\mathbf{Z}/N\mathbf{Z})^*$，使得

$$\mathrm{Log}_{\mathscr{P}}\varphi_Q(w)=uPr\circ\psi(w)\quad(\text{对每个 } w\in W).$$

由于 W 是 G-模，φ_Q和 ψ 均为 G-模同态，并且 G 在 Q 的所有 F-素理想因子上是可迁的. 由注记3.1.4即知 $\varphi_Q(w)=u\psi(w)\mathscr{P}$（对每个 $w\in W$）. 这就表明了满足条件(3). 从而证明了定理

3.2.2. ▌

§3.3 分圆单位和理想类群

本节需要有限群 G 的整表示的一些知识. 设 χ 是 G 在 l 进域 $\mathbf{Q}_l$ 上的不可约表示, $m=\dim\chi$ 是表示的维数, 则表示空间必存在一个格 L, 使得

$$\chi: G \to GL_m(\mathbf{Z}_l) = \mathrm{Aut}(L)$$

为群同态. 由于已假定 $(l, |G|)=1$, 所以

$$e(\chi) = \frac{1}{|G|}\sum_{\gamma\in G} T_r(\chi(\gamma))\gamma^{-1} \in \mathbf{Z}_l[G]$$

称作 χ-幂等元, 则对每个 G-模 Y, $Y\otimes_Z \mathbf{Z}_l$ 为 $\mathbf{Z}_l[G]$-模, 记 $Y(\chi)=e(\chi)(Y\otimes_Z \mathbf{Z}_l)$, 则

$$Y\otimes_Z \mathbf{Z}_l = \bigoplus_{\chi\in \hat{G}} Y(\chi),$$

其中 $\hat{G}$ 为 G 在域 $\mathbf{Q}_l$ 上的不可约表示全体, 而 $e(\chi)\mathbf{Z}_l[G]$ 同构于 $\mathbf{Q}_l$ 的 m 次不分歧扩域的整数环.

我们还需要下面的引理(函数域中 Minkowski 单位的存在性):

引理3.3.1 设 L/k 是有限伽罗华扩张, B 是 R 在 L 中的整闭包. 则存在环 B 中一个单位 ε, 使得由 $\{\varepsilon^\sigma: \sigma\in\mathrm{Gal}(L/k)\}$ 生成的群在 B 的单位群中的指数为有限的.

证明 令 $\infty_1, \cdots, \infty_g$ 是 L 的全部无限素除子, D 是 ∞_1 在 $\mathrm{Gal}(L/k)$ 中的分解群, $\sigma_1, \cdots, \sigma_g$ 是 $\mathrm{Gal}(L/k)$ 对于 D 的陪集代表元, 使得 $\infty_i=\sigma_i(\infty_1)$ $(1\leqslant i\leqslant g)$. 由于 L 的零次除子类群是有限的, 所以存在 B 中的单位 ε 在 ∞_1 处是零点, 而在 ∞_i 处 $(2\leqslant i\leqslant g)$ 均是极点. 以 v_{∞_i} 表示对于 ∞_i 的标准指数赋值, 则 $g-1$ 阶方阵

$$\left(v_{\infty_i}(\varepsilon^{\sigma_j})\right)_{1\leqslant i,j\leqslant g-1}$$

是可逆的, 所以 ε 即为所求. ▌

推论3.3.2 设 U^+ 是 $F=k(\Lambda_M)^+$ 的单位群, $k=\mathbf{F}_q(T)$,

$(l,q\Phi(M))=1$，$\chi(\neq 1)$为$G=\mathrm{Gal}(F/k)$在$\mathbf{Q}_l$上的不可约表示，则$U^+(\chi)$是秩为1的自由$e(\chi)\mathbf{Z}_l[G]$-模.

证明 由Dirichlet单位定理，$U^+\otimes_Z\mathbf{Z}_l$是秩$|G|-1$的自由$\mathbf{Z}_l$-模，并且$U^+\otimes_Z\mathbf{Z}_l=\bigoplus_{\chi\in\hat{G}}U^+(\chi)$. 取$\varepsilon$为$U^+$中的Minkowski单位，即$[U^+:\langle\varepsilon^\sigma:\sigma\in G\rangle]$有限，则$\{\varepsilon^\sigma:\sigma\neq 1\}$是$\mathbf{Z}$-线性无关的，从而也是$\mathbf{Z}_l$-线性无关的. 因此

$$e(\chi)\varepsilon=1\Longleftrightarrow\prod_{\sigma\in G}\sigma(\varepsilon)^{T_r(\chi(\sigma^{-1}))}=1$$

$$\Longleftrightarrow T_r(\chi(\sigma))=T_r(\chi(1))=m\quad(\forall\ \sigma\in G)$$

$$\Longleftrightarrow e(\chi)=e(1)\Longleftrightarrow\chi=1.$$

所以当$\chi\neq 1$时，$e(\chi)\varepsilon\neq 1$. 由于$e(\chi)\mathbf{Z}_l[G]$是$\mathbf{Z}_l$-秩为$m=\dim\chi$的离散赋值环，且与$\mathbf{Z}_l$有相同的素元，所以$U^+(\chi)$是无挠的秩为1的$e(\chi)\mathbf{Z}_l[G]$-模. ▌

下面证明我们的主要结果：

定理3.3.3 设$k=\mathbf{F}_q(T)$，$F=k(\Lambda_M)^+$，$G=\mathrm{Gal}(F/k)$，χ是G的$\mathbf{Q}_l$上不可约特征，$(l,q\Phi(M))=1$. U^+和C^+分别是F的单位群和(Sinnott)分圆单位群，Δ为F的理想类群的l-部分，则

$$|\Delta(\chi)|=|(U^+/C^+)(\chi)|.$$

证明 当$\chi=1$时，有

$$e(\chi)=\frac{1}{|G|}\sum_{\gamma\in G}\gamma=\frac{1}{|G|}\cdot\mathrm{Norm},$$

所以$|\Delta(1)|=|(U^+/C^+)(1)|=1$，即定理对$\chi=1$成立. 以下设$\chi\neq 1$，取$N=l\cdot|U^+/C^+(\chi)|\cdot|\Delta(\chi)|$，由于

$$e(\chi)(U^+/(U^+)^N)\cong e(\chi)(U^+/(U^+)^N\otimes\mathbf{Z}_l)$$

$$\cong e(\chi)(U^+\otimes\mathbf{Z}_l/(U^+)^N\otimes\mathbf{Z}_l)$$

$$\cong(e(\chi)(U^+\otimes\mathbf{Z}_l))/(e(\chi)(U^+\otimes\mathbf{Z}_l))^N,$$

而推论3.3.2表明$e(\chi)(U^+\otimes\mathbf{Z}_l)$是秩为1的自由$e(\chi)\mathbf{Z}_l[G]$-模，所以$e(\chi)(U^+/(U^+)^N)$是循环$e(\chi)\mathbf{Z}_l[G]$-模，设$\eta'^{-1}$是其生成元，则$\eta'^{-1}$的阶为$N$.

考虑$e(\chi)(U^+/(U^+)^N)$的子模$e(\chi)(C^+/(U^+)^N)$（注意，由

N 的取法可知 $C^+(\chi)\geqslant(U^+)^N(\chi))$. 则一定存在 $t\mid N$,使得 $e(\chi)(C^+/(U^+)^N)=\eta^{(q-1)}e(\chi)\mathbf{Z}_t[G]$. 从而 $e(\chi)\eta^{(q-1)}$的代表元可取成分圆单位(仍记为 $e(\chi)\eta^{(q-1)}$),并且

$$|U^+/C^+(\chi)|=[(U^+/(U^+)^N)(\chi):C^+/(U^+)^N(\chi)]=t^{\dim(\chi)}.$$

任取 $\Delta(\chi)$中一个元素 $\hat{u}_1$,令 W 是由 $e(\chi)\eta^{(q-1)}\in F^*/(F^*)^N$ 生成的 G-模,定义 G-模同态:

$$\psi:W\to\mathbf{Z}/N\mathbf{Z}[G],$$

使得 $\psi(e(\chi)\eta^{(q-1)})=t\cdot 1_G$. 由定理3.2.2知,存在 F 的一个素理想 $\mathscr{P}_1$为理想类 $\hat{u}_1$的代表元. 如果 $Q_1=\mathscr{P}_1\cap R\in S_N$, 从而有 $u\in(\mathbf{Z}/N\mathbf{Z})^*$,使得

$$\varphi_{Q_1}(e(\chi)\eta^{(q-1)})=ut\mathscr{P}_1.$$

由 §3.1可知道,考虑从 $e(\chi)\eta^{(q-1)}$开始的欧拉系,得到 $K_{Q_1}\in F^*/(F^*)^N$,使得在 I/NI 中,有

$$[K_{Q_1}]=[K_{Q_1}]_{Q_1}=\varphi_{Q_1}(e(\chi)\eta^{(q-1)})=ut\mathscr{P}_1.$$

如果 K_{Q_1}在 $F^*/(F^*)^N$ 中的阶为 m_1, $t_1=\dfrac{N}{m_1}$,则有 $f_1\in F^*$,使得 $K_{Q_1}=f_1^{t_1}$. 于是 $t_1\mid t$,并且在 $I\Big/\dfrac{N}{t_1}I$ 中$[f_1]=\dfrac{ut}{t_1}\mathscr{P}_1$. 由于$\dfrac{N}{t_1}$零化 $\Delta(\chi)$,所以在 $\Delta(\chi)$中$\dfrac{t}{t_1}\hat{u}_1=0$.

于是我们可以归纳地给出 $\Delta(\chi)$中元素 $\hat{u}_1,\cdots,\hat{u}_i$,并且素理想 $\mathscr{P}_\lambda$ 是理想类 $\hat{u}_\lambda$ 中的代表元,使得 $Q_\lambda=\mathscr{P}_\lambda\cap R$ $(1\leqslant\lambda\leqslant i)$均为 S_N 中的元素. 若 $J_i=\prod_{j=1}^{i}Q_j\in S_N$,则 $K_{J_i}\in F^*/(F^*)^N$. 令 W 是由 K_{J_i} 生成的 G-模,并且 K_{J_i}在 $F^*/(F^*)^N$ 中的阶为 m_i,令 $t_i=N/m_i$. 作 G-模同态 $\psi:W\to\mathbf{Z}/N\mathbf{Z}[G]$,使 $\psi(K_{J_i})=t_i1_G$. 取 $\hat{u}_{i+1}\in\Delta(\chi)-\langle\hat{u}_1,\cdots,\hat{u}_i\rangle$,这里$\langle\hat{u}_1,\cdots,\hat{u}_i\rangle$是由 $\hat{u}_1,\cdots,\hat{u}_i$ 生成的 G-模. 由定理3.2.2知,存在 F 中的素理想 $\mathscr{P}_{i+1}$是理想类 $\hat{u}_{i+1}$的代表元. 若 $Q_{i+1}=\mathscr{P}_i\cap R\in S_N$,则存在 $u\in(\mathbf{Z}/N\mathbf{Z})^*$,使得

$$\varphi_{Q_{i+1}}(K_{J_i})=ut_i\mathscr{P}_{i+1}.$$

令 $J_{i+1}=J_i\cdot Q_{i+1}\in S_N$，考虑从 $e(\chi)\eta^{(q-1)}$ 开始的欧拉系，得到 $K_{J_{i+1}}\in F^*/(F^*)^N$，并且

$$[K_{J_{i+1}}]=[K_{J_{i+1}}]_{Q_{i+1}}+\sum_{j\leqslant i}[K_{J_{i+1}}]_{Q_j}$$

$$=\varphi_{Q_{i+1}}(K_{J_i})+\sum_{j\leqslant i}[K_{J_{i+1}}]_{Q_j},$$

在 $I/(NI,I_{Q_1},\cdots,I_{Q_i})$ 中上式为 $[K_{J_{i+1}}]=ut_i\mathscr{P}_{i+1}$.

另一方面，设 $K_{J_{i+1}}$ 在 $F^*/(F^*)^N$ 中的阶为 m_{i+1}，令 $t_{i+1}=N/m_{i+1}$，则存在 $f_{i+1}\in F^*$，使得 $K_{J_{i+1}}=f_{i+1}^{t_{i+1}}$. 于是 $t_{i+1}\mid t_i$，并且在 $I\Big/\left(\frac{N}{t_{i+1}}I,I_{Q_1},\cdots,I_{Q_i}\right)$ 中 $[f_{i+1}]=u\,\frac{t_i}{t_{i+1}}\mathscr{P}_{i+1}$. 注意到 $t_{i+1}\mid t$，所以 N/t_{i+1} 零化 $\Delta(\chi)$，因此在 $\Delta(\chi)/\langle\hat{u}_1,\cdots,\hat{u}_i\rangle$ 中 $\frac{t_i}{t_{i+1}}\hat{u}_{i+1}=0$.

以上过程不妨设在第 k 步结束，即 $\Delta(\chi)=\langle\hat{u}_1,\cdots,\hat{u}_k\rangle$，这时

$$[\langle\hat{u}_1,\cdots,\hat{u}_{i+1}\rangle:\langle\hat{u}_1,\cdots,\hat{u}_i\rangle]\,\Big|\,(t_i/t_{i+1})^{\dim\chi}.$$

所以 $|\Delta(\chi)|\,\Big|\,(t/t_k)^{\dim\chi}$，这就表明 $|\Delta(\chi)|\,\Big|\,|(U^+/C^+)(\chi)|$.

另一方面，根据定理2.3.1及其注记，我们有

$$\prod_{\chi\in\hat{G}}|\Delta(\chi)|=|\Delta|=|(U^+/C^+)\otimes\mathbf{Z}_l|=\prod_{\chi\in\hat{G}}|(U^+/C^+)(\chi)|.$$

所以对每个 χ，必须 $|\Delta(\chi)|=|U^+/C^+(\chi)|$. 这就证明了定理3.3.3. ▌

注记 近来徐飞和赵健强把定理3.3.3推广到任意函数域上，其中分圆单位改用了 Hayes 引入的椭圆单位.

第 4 章

类数整除性

在上世纪中期，Kummer 在研究费马猜想时，对于分圆数域 $Q(\zeta_p)$ ($\zeta_p = e^{\frac{2\pi i}{p}}$，$p$ 为奇素数)的理想类数 h_p 给出了下列结果：记 h_p^+ 为 $Q(\zeta_p)^+ = Q(\zeta_p + \bar{\zeta}_p)$ 的理想类数，$h_p^- = h_p / h_p^+$，则 $h_p^- \in \mathbf{Z}$. 并且当 $p \geqslant 5$ 时，

$p \mid h_p \Leftrightarrow p \mid h_p^- \Leftrightarrow p$ 除尽某个 B_{2i} $\left(1 \leqslant i \leqslant \frac{p-3}{2}\right)$ 的分子，这里 B_n 是由下式定义的有理数(称为 Bernoulli 数)：

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n.$$

当 $p \nmid h_p$ 时，称 p 为正规素数，否则，p 称为非正规素数. Kummer 证明了：对于正规素数 p，方程

$$x^p + y^p = z^p$$

没有正整数解(x, y, z)，即费马猜想对于指数 p 是正确的. 已经知道，非正规素数有无穷多个，猜想正规素数也有无穷多个，但是这个问题至今尚未解决. 此外，Vandiver 猜想对每个 $p \geqslant 3$ 均有 $p \nmid h_p^+$，这个猜想至今也未解决.

后来，Herbrand 和 Ribet 证明了比 Kummer 更精细的结果. 以 A 表示 $Q(\zeta_p)$ 的理想类群的 Sylow$p$-子群，它可自然看成是 $\mathbf{Z}_p[G]$-模，其中

$$G = \mathrm{Gal}(Q(\zeta_p)/Q) = \{\sigma_a : a \in (\mathbf{Z}/p\mathbf{Z})^*\}.$$

而自同构 σ_a 是由 $\sigma_a(\zeta_p) = \zeta_p^a$ 所给出的. 由于 G 是 $p-1$ 阶循环群，所以 G 的每个特征的取值均是 $p-1$ 次单位根，从而特征取值可

以看成是 p-adic 整数环 $\mathbf{Z}_p$ 中的元素. 事实上, G 的 p-adic 特征群

$$\hat{G}=\mathrm{Hom}(G,\mathbf{Z}_p)$$

是由 Teichmüller 特征 $\omega: G\to\mathbf{Z}_p$ 所生成的 $p-1$ 阶循环群, 即 $\hat{G}=\{\omega^i: 0\leqslant i\leqslant p-2\}$, 其中 ω 由

$$\omega(a)\equiv a \pmod p \quad (a\in(\mathbf{Z}/p\mathbf{Z})^*)$$

所决定, 此处我们把 $\omega(\sigma_a)$ 记成 $\omega(a)$.

$\mathbf{Z}_p[G]$ 有正交幂等元素:

$$\varepsilon_i=\frac{1}{p-1}\sum_{a=1}^{p-1}\omega^i(a)\sigma_a^{-1} \quad (0\leqslant i\leqslant p-2),$$

对应地给出 $\mathbf{Z}_p[G]$-模 A 的直和分解:

$$A=\bigoplus_{i=0}^{p-2}A_i, \quad A_i=\varepsilon_iA.$$

而 $A^+=\bigoplus_{\substack{i=0\\2|i}}^{p-2}A_i$ 和 $A^-=\bigoplus_{\substack{i=0\\2\nmid i}}^{p-2}A_i$ 的阶分别是 h_p^+ 和 h_p^- 的 p 部分. 易知 $|A_0|=|A_1|=1$. 1923 年, Herbrand 证明了: 当 $p\geqslant5$ 时, 对于每个 $i=3,5,\cdots,p-2$, 有

$$|A_i|\neq1\Rightarrow p \text{ 除尽 } B_{p-i} \text{ 的分子}.$$

1976 年, Ribet 证明了此结果的逆命题⇐也成立. 对于以上所述可参见文献[57].

本章的主要目的是介绍 Kummer 的上述理论在分圆函数域中的两种模拟方式(分别对于分圆函数域的除子类数和理想类数). 对于除子类数, 类比于 Bernoulli 数 B_n, D. Goss 引进了一批多项式 $\beta_n(T)\in\boldsymbol{F}_q[T]$. 对于 $\boldsymbol{F}_q[T]$ 中每个首 1 不可约多项式 P, 以 h_P 和 h_P^+ 分别表示分圆函数域 $k(\Lambda_P)$ 和 $k(\Lambda_P)^+$ 的除子类数, $h_P^-=h_P/h_P^+$, 而以 p 表示域 $k=\boldsymbol{F}_q(T)$ 的特征. Goss 证明了: $p|h_P^+$ 和 $p|h_P^-$ 分别等价于 P 除尽某个多项式 $\beta_n(T)$ (确切的叙述为定理 4.1.5). 我们将在 §4.1 中介绍 Goss 的这个结果. 类似于数域的情形, 我们把满足 $p\nmid h_P^-$ 和 $p\nmid h_P^+$ 的 P 分别称为*第一类正规多项式*和*第二类正规多项式*. 在 §4.2 中要证明这两种非正规多项式均有无限多个. 特别地, Vandiver 猜想的模拟 $p\nmid h_P^+$ 是不正确

的. 在 § 4. 3 中对于二次不可约多项式 P 的正规性作更深入的讨论.

对于分圆函数域 $K^+=k(\Lambda_P)^+$ 的理想类数 $h(O_K)^+$, Okada[48] 发现早在 30 年代 Carlitz 研究的一批有理函数 $B_m(T)\in k(T)$ 就起着 Bernoulli 数的作用. Okada 证明了: $p\,|\,h(O_K)^+$ 当且仅当 P 除尽某个 B_m 的分子(详见定理 4. 5. 5). 我们将在 § 4. 4 和 § 4. 5 中介绍 Bernoulli-Carlitz 数 B_m 和 Okada 的结果. 最后, 在 § 4. 6 中利用分圆单位给出循环函数域理想类数的一些整除性的初等判别法.

§ 4. 1 Goss 的 zeta 函数和 Bernoulli-Goss 多项式

在 1983 年, D. Goss[25] 考虑了黎曼 zeta 函数

$$\zeta(s)=\sum_{n=1}^{\infty}n^{-s}$$

在函数域上的一种新的模拟(在这之前, 由于每个函数域等同于有限域上的射影代数曲线, 已经构作了 Hasse-Weil 的 zeta 函数). 我们知道, 当 s 是大于 1 的实数时, 级数 $\sum_{n=1}^{\infty}n^{-s}$ 对于通常的实数域拓扑是收敛的, 从而 $\zeta(s)\in\boldsymbol{R}$, 其中 $\boldsymbol{R}$ 表示实数域, 即有理数域 $\boldsymbol{Q}$ 对于通常拓扑的完备化域. 现在考虑有理函数域 $k=\boldsymbol{F}_q(T)$ 对于无限素除子 $\infty=\left(\frac{1}{T}\right)$ 的完备化域

$$k_\infty=\boldsymbol{F}_q\left(\left(\frac{1}{T}\right)\right),$$

类比于 $\mathbf{Z}$, 我们有多项式环 $R=\boldsymbol{F}_q[T]$, 而正整数集合的模拟是 R 中全体首 1 多项式构成的集合 R_1. 所以作为黎曼 zeta 函数的模拟, Goss 考虑了级数

$$\zeta_\infty(s)=\sum_{A\in R_1}A^{-s}=\sum_{n=0}^{\infty}a_n(s),\qquad(4.1.1)$$

其中

$$a_n(s) = \sum_{\substack{A\in R_1\\ \deg A=n}} A^{-s}.$$

我们用 $v=v_\infty$ 表示 k_∞ 中的 ∞-adic 标准指数赋值，即 $v\left(\frac{1}{T}\right)=1$. 若 s 是正整数，则当 $\deg A=n$ 时，$v(A^{-s})=sn$. 于是当 $n\to+\infty$ 时，

$$v(a_n(s)) \geqslant sn \to \infty.$$

这表明级数(4.1.1)对于 ∞-adic 拓扑是收敛的，即对每一个正整数 s，定义出 $\zeta_\infty(s)\in k_\infty$. 进而易知 $\zeta_\infty(0)=1$(注意 k_∞ 是特征 p 域，其中 $p|q$. 所以当 $n\geqslant 1$ 时，

$$a_n(0) = \sum_{\substack{A\in R_1\\ \deg A=n}} 1 = q^n = 0).$$

对于负整数 s，下面的引理表明 $\zeta_\infty(s)$ 事实上为多项式.

引理 4.1.1 设 K 为 $\boldsymbol{F}_q$ 的扩域，W 是 K 中有限维 $\boldsymbol{F}_q$-向量空间，则对于每个 $x\in K$，当正整数 $m<(q-1)\dim W$ 时，均有

$$\sum_{w\in W}(x+w)^m = 0.$$

证明 记 $n=\dim W$，取 W 的一组 $\boldsymbol{F}_q$-基 $e_1,\cdots,e_n$，则

$$\sum_{w\in W}(x+w)^m = \sum_{\alpha_1,\cdots,\alpha_n\in \boldsymbol{F}_q}(x+\alpha_1e_1+\cdots+\alpha_ne_n)^m$$

$$= \sum_{\substack{0\leqslant i_0,\cdots,i_n\leqslant m\\ i_0+\cdots+i_n=m}}\binom{m}{i_0,\cdots,i_n} x^{i_0}e_1^{i_1}\cdots e_n^{i_n}\sum_{\alpha_1\in \boldsymbol{F}_q}\alpha_1^{i_1}\cdots\sum_{\alpha_n\in \boldsymbol{F}_q}\alpha_n^{i_n},$$

其中 $\binom{m}{i_0,\cdots,i_n}=\frac{m!}{i_0!\ \cdots i_n!}$，并且定义 $0^0=1$.

由于 $i_0+\cdots+i_n=m<(q-1)n$，可知必有某个 $j(1\leqslant j\leqslant n)$，使得 $0<i_j<q-1$，于是 $\sum_{\alpha_j\in \boldsymbol{F}_q}\alpha_j^{i_j}=0\in K$(注意在 K 中 $q=0$). 这就表明了 $\sum_{w\in W}(x+w)^m=0$. ▌

由于

$$\{A\in R_1:\deg A=n\}$$
$$=\{T^n+a_1T^{n-1}+\cdots+a_n:a_1,\cdots,a_n\in \boldsymbol{F}_q\},$$

在引理 4.1.1 中取 $K=k=\boldsymbol{F}_q(T)$，而 W 是以 $1,T,T^2,\cdots,T^{n-1}$ 为基的 $\boldsymbol{F}_q$-向量空间，可知对每个正整数 m，当 $n>\frac{m}{q-1}$ 时，有

$$a_n(m)=\sum_{\substack{A\in R_1\\ \deg A=n}}A^m=\sum_{w\in W}(T^n+w)^m=0.$$

所以 $\zeta_\infty(s)$ 在负整数 $-m$ 处的取值

$$\zeta_\infty(-m)=\sum_{\substack{A\in R_1\\ \deg A\leqslant\frac{m}{q-1}}}A^m$$

是 $\boldsymbol{F}_q[T]$ 中的多项式.

黎曼把 $\zeta(s)=\sum\limits_{n\geqslant 1}n^{-s}$ 解析开拓成整个复平面 $\boldsymbol{C}$ 上的亚纯函数，而 Goss 把前面在 $\boldsymbol{Z}$ 上定义的 $\zeta_\infty(s)$ 构成拓扑群

$$S=k_\infty^*\times\boldsymbol{Z}_p$$

上的"亚纯"函数，其中 p 是 k_∞ 的特征，乘法群 k_∞^* 和加法群 $\boldsymbol{Z}_p$ 分别赋以 ∞-adic 和 P-adic 拓扑，而 S 采用它们的积拓扑. 以下记 $\pi=\frac{1}{T}$，对每个 $A\in R_1$，有 $A=T^n+a_1T^{n-1}+\cdots+a_n$，$n=\deg A$，

记
$$\langle A\rangle=\pi^{\deg A}A=1+a_1\pi+\cdots+a_n\pi^n,$$

于是 $\langle A\rangle\equiv 1\pmod{\pi}$. 所以对每个 $a\in\boldsymbol{Z}_p$，$\langle A\rangle^a$ 是可定义的，并且为 k_∞ 中元素. 现在对每个 $s=(s_0,s_1)\in S=k_\infty^*\times\boldsymbol{Z}_p$，定义

$$A^s=s_0^{\deg A}\langle A\rangle^{s_1}\in k_\infty,$$

而新的 Goss zeta 函数定义为

$$\tilde{\zeta}_\infty(s)=\tilde{\zeta}_\infty(s_0,s_1)=\sum_{A\in R_1}A^{-s}=\sum_{n\geqslant 0}\sum_{\substack{A\in R_1\\ \deg A=n}}A^{-s},\quad(4.1.2)$$

对每个整数 i，我们有 S 中的元素 $\varphi(i)=(\pi^{-i},i)$，这时

$$A^{\varphi(i)}=(\pi^{-i})^{\deg A}\langle A\rangle^i=\pi^{-i\deg A}\langle A\rangle^i=A^i,$$

于是
$$\zeta_\infty(i)=\tilde{\zeta}_\infty(\varphi(i)).$$

在这种意义下，可以把 $\tilde{\zeta}_\infty$ 看成是 ζ_∞ 的扩充. 为了证明 S 上的函数 $\tilde{\zeta}_\infty$ 有好的性质，我们需要如下引理：

引理 4.1.2　设 K 是 $\boldsymbol{F}_q$ 的扩域，并且 K 具有标准离散指数

赋值 v. 又设 W 是 K 中有限维 $\boldsymbol{F}_q$-向量空间，并且对每个 $w\in W$，均有 $v(w)\geqslant 1$. 对每个正整数 j，定义 W 的 $\boldsymbol{F}_q$-向量子空间

$$W_j=\{w\in W: v(w)\geqslant j\},$$

则对每个 $i\in\boldsymbol{Z}_p$ （p 是域 K 的特征)，均有

$$v\Big(\sum_{w\in W}(1+w)^i\Big)\geqslant(q-1)\sum_{j\geqslant 1}\dim W_j.$$

证明 由于函数 $\boldsymbol{Z}_p\mapsto K, i\mapsto(1+w)^i$ 是连续的，并且正整数集合是 $\boldsymbol{Z}_p$ 的稠密子集，所以只需对 i 为正整数的情形证明即可. 由于 $W=W_1\supseteq W_2\supseteq\cdots$，我们可以取 W 的一组 $\boldsymbol{F}_q$-基 $e_1,\cdots,e_n$ $(n=\dim W)$，使得它的前 $\dim W_j$ 个是 W_j 的一组基. 设 r 为正整数，使得 $W_r\neq(0), W_{r+1}=(0)$，则对每个 $1\leqslant j\leqslant r$，有 $W_j=W_{j+1}\oplus W'_j$，其中 W'_j 是以 $\{e_\lambda:\dim W_{j+1}+1\leqslant\lambda\leqslant\dim W_j\}$ 为基的向量空间. 于是对每个正整数 i，有

$$\sum_{w\in W}(1+w)^i=\sum_{\substack{w_j\in W'_j\\1\leqslant j\leqslant r}}(1+w_1+\cdots+w_r)^i$$

$$=\sum_{\substack{i_0,\cdots,i_r\geqslant 0\\i_0+\cdots+i_r=i}}\binom{i}{i_0,\cdots,i_r}\sum_{\substack{w_j\in W'_j\\1\leqslant j\leqslant r}}w_1^{i_1}\cdots w_r^{i_r}.$$

由引理 4.1.1 可知，当 $i<(q-1)\dim W'_j$ 时，$\sum\limits_{w\in W'_j}w^i=0$. 而当 $i\geqslant(q-1)\dim W'_j$ 时，

$$v\Big(\sum_{w\in W'_j}w^i\Big)\geqslant ij\geqslant(q-1)j\dim W'_j.$$

于是

$$v\Big(\sum_{w\in W}(1+w)^i\Big)\geqslant(q-1)\sum_{j=1}^{r}j\dim W'_j$$

$$=(q-1)\sum_{j=1}^{r}j(\dim W_j-\dim W_{j+1})$$

$$=(q-1)\sum_{j=1}^{r}\dim W_j.\qquad\blacksquare$$

定理 4.1.3 $\xi_\infty(s)$是 $S=k_\infty^*\times\boldsymbol{Z}_p$ 上的全纯函数.

证明 对每个 $s=(s_0,s_1)\in k_\infty^*\times \mathbf{Z}_p$，$A\in R_1$，显然

$$A^{-s}=s_0^{-\deg A}\langle A\rangle^{-s_1}$$

是 s 的全纯函数. 所以我们只需证明由(4.1.2)式定义的级数 $\zeta_\infty(s)$ 收敛即可. 我们有

$$\zeta_\infty(s)=\sum_{n\geqslant 0}s_0^{-n}c_n(s_1),$$

其中(记 $\pi=\frac{1}{T}$)

$$c_n(s_1)=\sum_{\substack{A\in R_1\\ \deg A=n}}\langle A\rangle^{-s_1}=\sum_{a_1,\cdots,a_n\in F_q}(1+a_1\pi+\cdots+a_n\pi^n)^{-s_1}.$$

在引理 4.1.2 中取 W 为 k_∞ 中由 $\pi,\pi^2,\cdots,\pi^n$ 张成的 F_q-向量空间，则

$$\dim W_j=n-j+1\quad(1\leqslant j\leqslant n+1).$$

所以由引理 4.1.2 得到

$$v(c_n(s_1))\geqslant(q-1)\sum_{j=1}^{n}(n-j+1)=(q-1)n(n+1)/2.$$

由于 $v(s_0^{-n})=nv(s_0^{-1})$ 是 n 的线性函数，所以当 $n\to+\infty$ 时，$v(s_0^{-n}c_n(s_1))\to+\infty$. 这就证明了级数(4.1.2)对每个 $s\in S$ 都收敛. ▌

定义 4.1.4 对每个整数 $i\geqslant 0$，定义 Bernoulli-Goss 多项式为

$$\beta_i(T)=\begin{cases}\zeta_\infty(\pi^i,-i)=\zeta_\infty(-i), & \text{若}(q-1)\nmid i;\\ \left.\dfrac{d\zeta_\infty(\pi^i x,-i)}{dx}\right|_{x=1}, & \text{若}(q-1)\mid i.\end{cases}$$

由 $\zeta_\infty(x,0)=1$ 可知 $\beta_0(T)=0$. 设 $i\geqslant 1$，则当 $(q-1)\nmid i$ 时，由引理 4.1.1 知

$$\beta_i(T)=\zeta_\infty(-i)=\sum_{\substack{A\in R_1\\ \deg A\leqslant i/(q-1)}}A^i\quad((q-1)\nmid i\geqslant 1),\tag{4.1.3}$$

而当 $(q-1)\mid i$ 时，

$$\bar{\zeta}_\infty(\pi^i x, -i) = \sum_{0\leqslant n\leqslant i/(q-1)} x^{-n} \sum_{\substack{A\in R_1\\ \deg A=n}} A^i.$$

于是

$$\beta_i(T) = -\sum_{\substack{A\in R_1\\ 1\leqslant\deg A\leqslant i/(q-1)}} A^i\deg A \quad ((q-1)|i). \quad (4.1.4)$$

所以 $\beta_i(T)$都是 $F_q[T]$中的多项式. 我们也可把(4.1.3)和(4.1.4)式作为 $\beta_i(T)$的定义. 下面的定理给出这些多项式的数论意义,可看作是分圆数域上的 Kummer 结果的一种模拟.

定理 4.1.5(Goss)　设 P 是 $F_q[T]$中首 1 不可约多项式,$d=\deg P$,$k=F_q(T)$, h_P 和 h_P^+ 分别是分圆函数域 $k(\Lambda_P)$和 $k(\Lambda_P)^+$的除子类数, $h_P^-=h_P/h_P^+$,p 为域 k 的特征. 则

$p|h_P^+\Leftrightarrow$存在 i,$1\leqslant i\leqslant q^d-2$,$(q-1)|i$,使得 $P|\beta_i(T)$;

$p|h_P^-\Leftrightarrow$存在 i,$1\leqslant i\leqslant q^d-2$,$(q-1)\nmid i$,使得 $P|\beta_i(T)$.

于是有 $P|h_P\Leftrightarrow$存在 i,$1\leqslant i\leqslant q^d-2$,使得 $P|\beta_i(T)$.

证明　群 $G=\mathrm{Gal}(k(\Lambda_P)/k)=\{\sigma_A: A\in(R/(P))^*\}$同构于$(R/(P))^*$,其中 $R=F_q[T]$. 而 $R/(P)\cong F_{q^d}$. 另一方面,以 ζ 表示复数域 C 中一个 q^d-1 次本原单位根,$q=p^\lambda$,熟知 p 在分圆数域 $Q(\zeta)$中剩余类域的次数 f 为满足 $p^s\equiv1 \pmod{q^d-1}$的最小正整数 s,即 $f=d\lambda$. 所以对环 $Z[\zeta]$的素理想 $\mathscr{P}|p$,有

$$Z[\zeta]/\mathscr{P}\cong F_{p^f}=F_{q^d}.$$

于是有域同构

$$\varphi: Z[\zeta]/\mathscr{P}\xrightarrow{\sim}R/(P).$$

熟知 $\bar{\zeta}$ 在$(Z[\zeta]/\mathscr{P})^*$中的阶为 q^d-1,从而 $\bar{A}=\varphi(\bar{\zeta})$ $(A\in R)$在$(R/P)^*$中的阶也为 q^d-1. 于是 $\hat{G}$ 中存在特征 ω,使得 $\omega(A)=\omega(\sigma_A)=\zeta$. 于是有

$$\varphi\omega(A)\equiv A \pmod P,$$

特征 ω 的阶为 q^d-1,因此它生成特征群 $\hat{G}$,即 $\hat{G}=\{\omega^i; 0\leqslant i\leqslant q^d-2\}$. 并且 ω^i 是实特征$\Leftrightarrow(q-1)|i$. 所以类数公式(定理1.5.2)给出了

$$h_P^+ = \prod_{\substack{1\leqslant i\leqslant q^d-2\\(q-1)|i}} h(\omega^i),\quad h_P^- = \prod_{\substack{1\leqslant i\leqslant q^d-2\\(q-1)\nmid i}} h(\omega^i),$$

其中

$$h(\omega^i) = \begin{cases} \sum_{A\in R_1}\omega^i(A), & 若(q-1)\nmid i; \\ -\sum_{A\in R_1}\omega^i(A)\deg A, & 若(q-1)|i. \end{cases}$$

由 $\varphi\omega^i(A)\equiv A^i \pmod{P}$和关于 $\beta_i(T)$的公式(4.1.3)和(4.1.4)便得到

$$\varphi h(\omega^i) \equiv \beta_i(T) \pmod{P},$$

于是

$p|h_P^+ \Leftrightarrow \mathscr{P}|h_P^+$

$\Leftrightarrow$ 存在 i，$1\leqslant i\leqslant q^d-2$，$(q-1)|i$，使得 $\mathscr{P}|h(\omega^i)$.

但是 $h(\omega^i)\in \mathbf{Z}[\zeta]$，而

$$\begin{aligned}\mathscr{P}|h(\omega^i) &\Leftrightarrow h(\omega^i) = 0 \in \mathbf{Z}[\zeta]/\mathscr{P}\\ &\Leftrightarrow \beta_i(T) = \varphi h(\omega^i) = 0 \in R/(P)\\ &\Leftrightarrow P|\beta_i(T).\end{aligned}$$

这就表明了

$p|h_P^+ \Leftrightarrow$存在 i，$1\leqslant i\leqslant q^d-2$，$(q-1)|i$，使得 $P|\beta_i(T)$. 类似可证明 $p|h_P^-$ 的情形.　▌

§4.2　不可约多项式的正规性

设 P 是 $\mathbf{F}_q[T]$中首1不可约多项式，p 是 $\mathbf{F}_q$ 的特征. 如果 $p\nmid h_P^-$ ($p\nmid h_P^+$)，则 P 称作*第1类(第2类)正规多项式*. 如果$p|h_P^-$ ($p|h_P^+$)，则 P 称作*第1类(第2类)非正规多项式*. 本节的目的是证明非正规多项式有无限多个(见定理4.2.5). 定理4.1.5表明了这个问题依赖于 Bernoulli-Goss 多项式 $\beta_i(T)$是否可被 P 整除. 下面先给出 $\beta_i(T)$的一些基本性质：

定理4.2.1　(1) 递推关系　$\beta_0(T)=0$，而对于 $i\geqslant 1$，有

$$\beta_i(T)=1-\sum_{\substack{b=0\\(q-1)|(i-b)}}^{i-1}\binom{i}{b}T^b\beta_b(T);$$

(2) $\beta_{pi}(T)=\beta_i(T)^p$;

(3) 同余关系 设 i、j、d 是正整数. 如果 $i\equiv j \pmod{q^d-1}$, 则

$$\beta_i(T)\equiv\beta_j(T)\pmod{T^{q^d}-T}.$$

特别是, 若 P 是 $F_q[T]$ 中 d 次首1不可约多项式, 则 i、$j\geqslant 1$, 并且 $i\equiv j \pmod{q^d-1}$ 时, 有

$$\beta_i(T)\equiv\beta_j(T)\pmod{P}.$$

证明 (1) 对每个 $n\geqslant 1$, 有

$$\sum_{\substack{A\in R_1\\ \deg A=n}}A^i=\sum_{\substack{B\in R_1\\ \deg B=n-1}}\sum_{a\in F_q}(BT+a)^i$$

$$=\sum_{b=0}^{i}\binom{i}{b}T^b\sum_B B^b\sum_a a^{i-b}.$$

当 $(q-1)\nmid(i-b)$ 和 $b=i$ 时, $\sum\limits_{a\in F_q}a^{i-b}=0$; 而当 $(q-1)|(i-b)\geqslant 1$ 时, $\sum\limits_{a\in F_q}a^{i-b}=q-1=-1$. 于是

$$\sum_{\substack{A\in R_1\\ \deg A=n}}A^i=-\sum_{\substack{b=0\\(q-1)|(i-b)}}^{i-1}\binom{i}{b}T^b\sum_{\substack{B\in R_1\\ \deg B=n-1}}B^b.$$

所以当 $(q-1)\nmid i$ 时,

$$\beta_i(T)=\sum_{A\in R_1}A^i=1+\sum_{n\geqslant 1}\sum_{\substack{A\in R_1\\ \deg A=n}}A^i$$

$$=1-\sum_{n\geqslant 1}\sum_{\substack{b=0\\(q-1)|(i-b)}}^{i-1}\binom{i}{b}T^b\sum_{\substack{B\in R_1\\ \deg B=n-1}}B^b$$

$$=1-\sum_{\substack{b=0\\(q-1)|(i-b)}}^{i-1}\binom{i}{b}T^b\beta_b(T).$$

而当 $(q-1)|i\geqslant 1$ 时, $(q-1)|(i-b)$ 相当于 $(q-1)|b$. 这时

$$\beta_i(T) = -\sum_{n\geqslant 1} n \sum_{\substack{A\in R_1 \\ \deg A = n}} A^i$$

$$= \sum_{n\geqslant 1}(n-1+1) \sum_{\substack{b=0 \\ (q-1)\mid b}}^{i-1} \binom{i}{b} T^b \sum_{\substack{B\in R_1 \\ \deg B = n-1}} B^b$$

$$= \sum_{\substack{b=0 \\ (q-1)\mid b}}^{i-1} \binom{i}{b} T^b \sum_{B\in R_1} B^b - \sum_{\substack{b=0 \\ (q-1)\mid b}}^{i-1} \binom{i}{b} T^b \beta_b(T).$$

当 $b=0$时，

$$\sum_{B\in R_1} B^b = \sum_{n\geqslant 1} \sum_{\substack{B\in R_1 \\ \deg B = n}} 1 = 1.$$

而当$(q-1)\mid b\geqslant 1$时，应用递推公式

$$\sum_{B\in R_1} B^b = 1 - \sum_{\substack{c=0 \\ (q-1)\mid c}}^{b-1} \binom{b}{c} T^c \sum_{B\in R_1} B^c$$

可知$\sum\limits_{B\in R_1} B^b = 0$. 于是

$$\beta_i(T) = 1 - \sum_{\substack{b=0 \\ (q-1)\mid b}}^{i-1} \binom{i}{b} T^b \beta_b(T) \quad (\text{当}(q-1)\mid i \geqslant 1\ \text{时}).$$

(2) 当$(q-1)\nmid i$时，由于域$\boldsymbol{k}=\boldsymbol{F}_q(T)$的特征为$p$，

$$\beta_{ip}(T) = \sum_{A\in R_1} A^{ip} = \Big(\sum_{A\in R_1} A^i\Big)^p = \beta_i(T)^p.$$

对于$(q-1)\mid i$的情形，类似可证明.

(3) 当i、$j\geqslant 1$，$i\equiv j \pmod{q^d-1}$时，则对每个$A\in R_1$，均有

$$A^i \equiv A^j \pmod{T^{q^d}-T}.$$

于是当$(q-1)\nmid i$时，有

$$\beta_i(T) = \sum_{A\in R_1} A^i \equiv \sum_{A\in R_1} A^j$$

$$= \beta_j(T) \pmod{T^{q^d}-T}.$$

对于$(q-1)\mid i$的情形，类似可证明. 最后一个论断是由于每个首1不可约d次多项式都是$T^{q^d}-T$的因子. 从而本定理得证. ∎

由定理4.1.5可知，计算$\beta_i(T)$的具体表达式和它的素因子分

解，对于研究除子类数 $h_F^{\pm}$ 的整除性是很重要的. 目前只对一些特殊的情形得到了 $\beta_i(T)$的具体表达式. 以下记 $s=q-1$，对于正整数 i 的 q-adic 展开式

$$i=\sum_{e\geqslant 0}c_e q^e \quad (0\leqslant c_e\leqslant q-1)$$

我们记 $l(i)=\sum_{e\geqslant 0}c_e\in\mathbf{Z}$. 易知 $l(i)\equiv i \pmod s$.

引理4.2.2 设 i 是正整数.

(1) 若 $l(i)\leqslant s$，则 $\beta_i(T)=1$；若 $l(i)\leqslant 2s$，则

$$\beta_i(T)=1-\sum_{1\leqslant j<i/s}\binom{i}{js}T^{i-js}.$$

(2) 若 $i=a+bq^e$ 为 q-adic 展开式，$e\geqslant 1$，并且 $l(i)=a+b\geqslant q$，记 $\rho=a+b-s(\geqslant 1)$，则

$$\beta_i(T)=1-\binom{b}{\rho}(T^{q^e}-T)^{\rho}.$$

证明 (1) 定理4.2.1中的递推公式可以写成

$$\beta_i(T)=1-\sum_{1\leqslant j<i/s}\binom{i}{js}T^{i-js}\beta_{i-js}(T). \qquad (4.2.1)$$

先设 $l(i)\leqslant s$，为证 $\beta_i(T)=1$，只需证明对每个 js $(1\leqslant js<i)$都有 $\binom{i}{js}\equiv 0 \pmod p$，这里 p 是 $\mathbf{F}_q$ 的特征. 设 $i=\sum a_e p^e$ 和 $js=\sum b_e p^e$ 是 p-adic 展开式，则 Lucas 定理是说

$$\binom{i}{js}\equiv\prod_e\binom{a_e}{b_e} \pmod p.$$

所以当$\binom{i}{js}\not\equiv 0 \pmod p$时，必然有 $b_e\leqslant a_e$(对每个 e). 由此可知

$$l(i)=l(i-js)+l(js)>l(js)\geqslant 1.$$

但是$l(js)\equiv js\equiv 0 \pmod s$. 于是$l(i)>l(js)\geqslant s$，这与假设$l(i)\leqslant s$相矛盾. 所以当 $l(i)\leqslant s$ 时，$\beta_i(T)=1$.

现在我们设 $l(i)\leqslant 2s$. 由(4.2.1)式可知道只需考虑$1\leqslant js<i$，

$\binom{i}{js}\not\equiv 0 \pmod{p}$ 的情形. 这时 $1 \leqslant l(js) < l(i) \leqslant 2s$. 但是 $l(is) \equiv 0 \pmod{s}$, 所以 $l(js) = s$. 于是

$$l(i - js) = l(i) - l(js) \leqslant 2s - s = s.$$

由前面所证可知 $\beta_{i-js}(T) = 1$. 代入(4.2.1)式, 得到

$$\beta_i(T) = 1 - \sum_{1 \leqslant j < i/s} \binom{i}{js} T^{i-js}.$$

(2) 由于 $l(i) = a + b \leqslant 2s$, 所以

$$\beta_i(T) = 1 - \sum_{1 \leqslant js < i} \binom{i}{js} T^{i-js}.$$

如果 $\binom{i}{js}\not\equiv 0 \pmod{p}$, $1 \leqslant js < i$, 上面已证 $l(js) = s$, 并且 js 的 q-adic展开式有 $js = (s-m) + mq^t$ 的形式, 其中 $s - a \leqslant m \leqslant b$. 于是

$$\beta_i(T) = 1 - \sum_{m=s-a}^{b} \binom{b}{m}\binom{a}{s-m} T^{(b-m)q^t + a + m - s}.$$

设 $a = \sum a_e p^e$ 和 $s - m = \sum b_e p^e$ 是 p-adic 展开式, 如果 $\binom{a}{s-m} \not\equiv 0 \pmod{p}$, 则 $0 \leqslant b_e \leqslant a_e \leqslant p - 1$ (对每个 e). 这时

$$\binom{a_e}{b_e}\binom{p-1-b_e}{p-1-a_e}^{-1} = \frac{a_e!(p-1-a_e)!}{b_e!(p-1-b_e)!} \equiv (-1)^{a_e - b_e} \pmod{p}.$$

于是有

$$\binom{a}{s-m} \equiv \prod_e \binom{a_e}{b_e} \equiv (-1)^{a+m-s} \prod_e \binom{p-1-b_e}{p-1-a_e} \equiv (-1)^{a+m-s}\binom{m}{s-a} \pmod{p}.$$

再利用恒等式

$$\binom{b}{\rho}\binom{\rho}{m+a-s} = \binom{b}{m}\binom{m}{s-a} \quad (\rho = a + b - s),$$

便得

$$\beta_i(T) = 1 - \sum_{m=s-a}^{b} (-1)^{a+m-s} \binom{b}{m} \binom{m}{s-a} T^{(b-m)q^t+a+m-s}$$

$$= 1 - \sum_{m=s-a}^{b} (-1)^{a+m-s} \binom{b}{\rho} \binom{\rho}{m+a-s} T^{(b-m)q^t+a+m-s}$$

$$= 1 - \binom{b}{\rho} \sum_{j=0}^{\rho} \binom{\rho}{j} (T^{q^t})^{\rho-j} (-T)^j \quad (\text{取 } j = m+a-s)$$

$$= 1 - \binom{b}{\rho} (T^{q^t} - T)^{\rho}. \qquad \blacksquare$$

例4.2.3 对于分圆数域的情形，Kummer 的结果表明了 $p \mid h_p^+ \Rightarrow p \mid h_p^-$，并且 Vandiver 猜想对每个奇素数 p 均有 $p \nmid h_p^+$. 对于分圆函数域 $k(\Lambda_p)$ 的情形，下面的例子表明了除子类数 h_P^+ 和 h_P^- 是否被 F_q 的特征 p 所能整除，是彼此独立的，并且所有可能的情形都会发生.

(1) 在例1.5.4(1)中给出了 $p \nmid h_P = h_P^+ h_P^-$ 的情形，其中 $p = q = 2$，$P = T^3 + T + 1 \in F_2[T]$，$h_P^- = 1$，$h_P^+ = 71$.

(2) 在例1.5.4(2)中给出了 $p \nmid h_P^+$，$p \mid h_P^-$ 的情形，其中 $p = q = 5$，$P = T^2 + 2 \in F_5[T]$，$h_P^+ = 1$，$h_P^- = 2^{10} \cdot 5^3$. 事实上，由引理4.2.2中的(2)可知

$$\beta_{18}(T) = 1 - \binom{3}{2} (T^5 - T)^2$$

$$= 1 - 3(T^5 - T)^2 \equiv 0 \pmod{T^2 + 2}.$$

从而由定理4.1.5也可得到 $p \mid h_P^-$.

(3) 当 $p = q = 2$ 时，对每个 $F_2[T]$ 中的首1不可约多项式 P，$[k(\Lambda_P) : k(\Lambda_P)^+] = q - 1 = 1$，即 $k(\Lambda_P) = k(\Lambda_P)^+$，于是 $h_P = h_P^+$，$h_P^- = 1$. 我们在以后将证明，存在无限多的 $P \in F_2[T]$，使得 $2 \mid h_P = h_P^+$（见下面的定理4.2.4）. 所以给出无限多的 P 满足 $p \nmid h_P^-$，$p \mid h_P^+$.

(4) 最后举一个 $p \mid h_P^+$ 同时 $p \mid h_P^-$ 的例子. 取 $p = q = 3$，$P = T^3 - T - 1 \in F_3[T]$，由引理4.2.2算出

$$\beta_5(T) = 1 - \binom{1}{1} (T^3 - T) = 1 - T^3 + T \equiv 0 \pmod{P},$$

$$\beta_8(T)=1-(T^3-T)^2\equiv 0 \pmod{P}.$$

再由定理4.1.5可知$3\mid h_P^+$，并且$3\mid h_P^-$.

定理4.2.4[14] 当$q=2$时，在$\boldsymbol{F}_2[T]$中存在无穷多个第2类非正规首1不可约多项式. 而对每个$q\geqslant 3$，在$\boldsymbol{F}_q[T]$中均存在无穷多个同时为第1类和第2类非正规的首1不可约多项式.

证明 我们只需证明：对每个固定的q和任意正整数n，$\boldsymbol{F}_q[T]$中均存在首1不可约多项式P和正整数$a=a(P)$，使得$a>\deg P>n$，并且

$$P\mid\beta_i(T)\quad (\text{对每个}\ i,1+(q-1)q^a\leqslant i\leqslant(q-1)(q^a+1)). \tag{4.2.2}$$

如果这个命题成立，由于n可任意大，可知$\boldsymbol{F}_q[T]$中满足(4.2.2)式的P有无穷多个. 利用定理4.1.5，取$i=(q-1)(q^a+1)$即知$p\mid h_P^+$(这里p是$\boldsymbol{F}_q$的特征)，于是这些P是第2类非正规的首1不可约多项式. 如果$q\geqslant 3$，取$i=j+(q-1)q^a$ $(1\leqslant j\leqslant q-2)$，可知$p\mid h_P^-$，即这些$P$也是第1类非正规的首1不可约多项式. 这就证明了定理4.2.4.

现在证明上述命题. 对于固定的q和n，在引理4.2.2(2)中取$i=j+(q-1)q^{n!}$ $(1\leqslant j\leqslant q-1)$，可知

$$\beta_i(T)=1-\binom{q-1}{j}(T^{q^{n!}}-T)^j=1-(T-T^{q^{n!}})^j. \tag{4.2.3}$$

由于$\boldsymbol{F}_q[T]$中次数不超过n的不可约多项式都是$T-T^{q^{n!}}$的因子，由(4.2.3)式可知在$\boldsymbol{F}_q[T]$中$\beta_{1+(q-1)q^{n!}}(T)$有次数大于n的首1不可约因子P. 记$d=\deg P(>n)$，并令a是满足$a\equiv n! \pmod{d}$的最小正整数，则$1\leqslant a<d$(注意，由$P\mid\beta_{1+(q-1)q^{n!}}(T)$和(4.2.3)式知$d\nmid n!$). 由同余性质(定理4.2.1(3))可知

$$\beta_{1+(q-1)q^a}(T)\equiv\beta_{1+(q-1)q^{n!}}(T)\equiv 0 \pmod{P}.$$

再由(4.2.3)式知

$$\beta_{1+(q-1)q^{n!}}(T)\mid\beta_{j+(q-1)q^{n!}}(T)\quad (1\leqslant j\leqslant q-1).$$

于是

$\beta_{j+(q-1)q^{d}}(T) \equiv \beta_{j+(q-1)q^{d+1}}(T) \equiv 0 \pmod{P} \quad (1 \leqslant j \leqslant q-1).$

这就完成了定理4.2.4的证明. ▌

注记 (1) Goss 和 Sinnott[38]利用近代算术代数几何工具证明了比定理4.1.5更精确的结果(相当于前面所述的关于分圆数域 $\boldsymbol{Q}(\zeta_p)$ 的 Ribet 结果):对于 $G=\mathrm{Gal}(k(\Lambda_P)/k)$的特征群 $\hat{G}=\{\omega^i:0\leqslant i\leqslant q^d-2\}$,以 A 表示 $k(\Lambda_P)$的除子类群的 Sylow p-子群,$A(\omega^i)$表示 A 的 ω^i-分支,则有直和分解:

$$A = A^+ \oplus A^-,\ A^+ = \bigoplus_{(q-1)\mid i} A(\omega^i),\ A^- = \bigoplus_{(q-1)\nmid i} A(\omega^i).$$

并且 A^+ 即是 $k(\Lambda_P)^+$ 的除子类群的 Sylow p-子群,即 $|A^+|$ 和 $|A^-|$分别是 h_P^+ 和 h_P^- 的 p-因子. 在文献[38]中证明了:对每个$1\leqslant i\leqslant q^d-2$, $|A(\omega^i)|\neq 1$当且仅当 $P\mid\beta_{q^d-1-i}(T)$. 利用这个结果,我们在定理4.2.4的证明中实际上得到了:对每个 $q\geqslant 3$,在 $\boldsymbol{F}_q[T]$中存在无穷多个首1不可约多项式 P, 使得 $p\mid h_P^+$ 并且 $p^{q-2}\mid h_P^-$.

(2) 目前对每个 q,我们不知道在 $\boldsymbol{F}_q[T]$中是否存在无穷多的第2类正规不可约多项式;当 $q\geqslant 3$时,也不知道在 $\boldsymbol{F}_q[T]$中是否存在无穷多的第1类正规的不可约多项式.

§4.3 二次不可约多项式的正规性

在本节中我们决定 $\boldsymbol{F}_q[T]$中二次首1不可约多项式的正规性. 当 q 为素数时,由 Ireland 和 Small 给出正规性判别法,对一般情形见文献[14].

我们固定 q,考虑 $\boldsymbol{F}_q[T]$中二次首1不可约多项式

$$P = T^2 + AT + B,\ k = \boldsymbol{F}_q(T),\ K = k(\Lambda_P).$$

由类数公式知

$$h_P^+ = \prod_{\substack{\chi\in\hat{K}^+\\ \chi\neq\chi_0}}\Big(-\sum_{a\in\boldsymbol{F}_q}\chi(T+a)\Big) = \prod_{\substack{\chi\in\hat{K}^+\\ \chi\neq\chi_0}} 1 = 1.$$

所以每个二次的 P 必是第2类正规的多项式. 我们的目的是给出 P 为第1类正规的判别法,设 $q=P^\lambda$,由前述可知:

P 为第1类正规的多项式$\Leftrightarrow p \nmid h_P^- = h_P$

$\Leftrightarrow P \nmid \beta_i(T)$ （对每个 $i, 1 \leqslant i \leqslant q^2-2$），

但是当$1 \leqslant i \leqslant q^2-2$时，$i$ 的 q-adic 展开有形式 $i=a+bq$. 这时 $\beta_i(T)$可以写出明显的形式（引理4.2.2）：

$$\beta_i(T) = 1 - \binom{b}{\rho}(T^q - T)^\rho,$$

其中 $\rho = a+b-(q-1) \geqslant 1$（当 $\rho \leqslant 0$时 $\beta_i(T)=1$）. 所以

P 为（第1类）正规的多项式

$$\Leftrightarrow \binom{b}{\rho}(T^q - T)^\rho \not\equiv 1 \pmod{P}$$

$$(1 \leqslant \rho \leqslant b \leqslant q-1,\ \rho < q-1). \tag{4.3.1}$$

如果把 T 改成 $T+\alpha$ （$\alpha \in \boldsymbol{F}_q$），则

$$(T+\alpha)^q - (T+\alpha) = T^q - T.$$

由（4.3.1）式知 $P(T)$和多项式 $P(T+\alpha)$有同样的正规性. 所以当 $p \geqslant 3$（即$2 \nmid q$）时，我们不妨设 $P=T^2-d$，由假定 P 是不可约的，可知 d 是 $\boldsymbol{F}_q^*$ 中非平方元素.

定理4.3.1 设 $q=p^\lambda$，P 为 $\boldsymbol{F}_q[T]$中首1不可约多项式.

(1) 当 $p=2$时，$P=T^2+AT+B$ 正规$\Leftrightarrow A$ 是 $\boldsymbol{F}_q^*$ 的乘法群生成元. 特别地，$\boldsymbol{F}_q[T]$中共有$\frac{1}{2}q \cdot \varphi(q-1)$个二次正规多项式（$\varphi(n)$表示欧拉函数）.

(2) 当 $p \geqslant 3$时，对于 $P=T^2-d$ （d 为 $\boldsymbol{F}_q^*$ 中非平方元素），则下列三个条件彼此等价：

$(2)_1$ P 是正规的；

$(2)_2$ $\binom{b}{2\rho}(4d)^\rho \neq 1 \in \boldsymbol{F}_q$ （对所有$2 \leqslant 2\rho \leqslant b \leqslant q-1$）；

$(2)_3$ $4d$ 为乘法群 $\boldsymbol{F}_q^*$ 的生成元，并且对于 $g=(4d)^{\frac{q-1}{p-1}}$和所有满足$2 \leqslant 2k \leqslant b_j \leqslant p-1$的整数 k 和 $b_0, b_1, \cdots, b_{\lambda-1}$，均有

$$g^k \prod_{j=0}^{\lambda-1} \binom{b_j}{2k} \neq 1 \in \boldsymbol{F}_p.$$

证明 (1) 当 $p=2$时，

$$(T^q - T)^2 \equiv T^{2q} - T^2 \equiv (AT+B)^q - (AT+B) = A(T^q - T) \pmod{P}.$$

由于 $P \nmid T^q - T$，所以 $T^q - T \equiv A \pmod{P}$. 由(4.3.1)式可知

$$P \text{ 正规} \Longleftrightarrow \binom{b}{\rho} A^\rho \not\equiv 1 \pmod{P}$$

$$(\text{对于 } 1 \leqslant \rho \leqslant b \leqslant q-1, \rho < q-1)$$

$$\Longleftrightarrow A^\rho \neq 1 \in \boldsymbol{F}_q^* \quad (\text{对每个 } 1 \leqslant \rho \leqslant q-2)$$

$$\Longleftrightarrow A \text{ 是 } \boldsymbol{F}_q^* \text{ 的生成元}.$$

熟知 $\boldsymbol{F}_q^*$ 共有 $\varphi(q-1)$个生成元，而对每个生成元 A，共有 $q/2$个 $B \in \boldsymbol{F}_q$使 T^2+AT+B 不可约. 所以 $\boldsymbol{F}_q[T]$中共有$\frac{1}{2}q \cdot \varphi(q)$个二次正规首1不可约多项式.

(2) 由于 d 是 $\boldsymbol{F}_q^*$ 中非平方元素，所以 $d^{\frac{q-1}{2}} \equiv -1 \pmod{p}$. 于是

$$T^{q-1} \equiv d^{\frac{q-1}{2}} \equiv -1 \pmod{P}, \quad T^q - T \equiv -2T \pmod{P}.$$

由(4.3.1)式可知，对于

$$P = T^2 - d \in \boldsymbol{F}_q[T] \quad (q = P^\lambda, p \geqslant 3),$$

有

$$P \text{ 正规} \Longleftrightarrow \binom{b}{\rho}(-2T)^\rho \not\equiv 1 \pmod{P}$$

$$(\text{对于 } 1 \leqslant \rho \leqslant b \leqslant q-1, \rho < q-1).$$

当$2 \nmid \rho$时，

$$\binom{b}{\rho}(-2T)^\rho = \binom{b}{\rho}(-2)^\rho T \cdot (T^2)^{\frac{\rho-1}{2}}$$

$$\equiv \binom{b}{\rho}(-2)^\rho d^{\frac{\rho-1}{2}} T \not\equiv 1 \pmod{P}.$$

而当 $\rho=b=q-1$时，

$$\binom{b}{\rho}(-2T)^\rho = T^{q-1} \equiv -1 \pmod{P}.$$

因此

$$P \text{ 正规} \Leftrightarrow \binom{b}{2\rho}(-2T)^{2\rho} \not\equiv 1 \pmod{P}$$

$$(\text{对于 } 2 \leqslant 2\rho \leqslant b \leqslant q-1).$$

$$\Leftrightarrow \binom{b}{2\rho}(4d)^{\rho} \not\equiv 1 \pmod{P}$$

$$(\text{对于 } 2 \leqslant 2\rho \leqslant b \leqslant q-1).$$

这就证明了$(2)_1$和$(2)_2$等价. 注意,若$(2)_2$成立,则$4d$ 必是 $\boldsymbol{F}_q^*$ 的生成元,于是 $g=(4d)^{\frac{q-1}{p-1}}$是 $\boldsymbol{F}_p^*$ 的生成元.

现在证明$(2)_2 \Rightarrow (2)_3$:如果$(2)_3$不成立,则有 k 和 b_j $(0\leqslant j\leqslant \lambda-1)$使得

$$g^k \prod_{j=0}^{\lambda-1}\binom{b_j}{2k} = 1 \in \boldsymbol{F}_p,\ 2 \leqslant 2k \leqslant b_j \leqslant p-1 \quad (0 \leqslant j \leqslant \lambda-1).$$

令

$$b = \sum_{j=0}^{\lambda-1} b_j p^j,\ 2\rho = 2k(q-1)/(p-1)$$

$$= 2k(1+p+p^2+\cdots+p^{\lambda-1}),$$

由 Lucas 定理知

$$\binom{b}{2\rho}(4d)^{\rho} = \prod_{j=0}^{\lambda-1}\binom{b_j}{2k} g^k = 1 \in \boldsymbol{F}_p.$$

这就和$(2)_2$相矛盾.

最后证明$(2)_3 \Rightarrow (2)_2$:如果$(2)_2$式不成立,则有 ρ 和 b 满足$2\leqslant 2\rho\leqslant b\leqslant q-1$,并且$\binom{b}{2\rho}(4d)^{\rho}=1\in \boldsymbol{F}_q$,于是$(4d)^{\rho}\in \boldsymbol{F}_p$. 但是$4d$ 为 $\boldsymbol{F}_q^*$ 的生成元,所以$\frac{q-1}{p-1}\Big|\rho$. 于是

$$\rho = k(q-1)/(p-1) = k(1+p+p^2+\cdots+p^{\lambda-1}),$$

其中 $k\leqslant \frac{p-1}{2}$ (因为$2\rho\leqslant q-1$). 设 b 的 p-adic 展开为 $b=\sum_{j=0}^{\lambda-1} b_j p^j$,则

$$g^k \prod_{j=0}^{\lambda-1} \binom{b_j}{2k} = \binom{b}{2\rho} (4d)^\rho = 1 \in \boldsymbol{F}_p.$$

这与$(2)_3$相矛盾. 这就完成了定理4.3.1的证明. ▌

注记 Ireland 和 Small 对于 $q=p\geqslant 3$的情形证明了$(2)_1$和$(2)_2$等价. 注意$(2)_3$只涉及基域 $\boldsymbol{F}_p$,所以我们有如下推论:

推论4.3.2 设 $q=p^n$, $q'=p^m$, $n>m$, $p\geqslant 3$. 如果 $\boldsymbol{F}_q[T]$中存在正规二次首1不可约多项式,则在 $\boldsymbol{F}_{q'}[T]$中也如此.

证明 设 P 为 $\boldsymbol{F}_q[T]$中正规二次首1不可约多项式. 不妨设 $P=T^2-\frac{d}{4}$. 由定理4.3.1知 d 是 $\boldsymbol{F}_q^*$ 的生成元,于是 $g=d^{\frac{q-1}{p-1}}$为 $\boldsymbol{F}_p^*$ 的生成元. 易知存在 $\boldsymbol{F}_{q'}^*$ 的生成元 d' 使得 $g=(d')^{\frac{q'-1}{p-1}}$. 再由定理4.3.1可知

$$T^2-\frac{d}{4}\text{在 } \boldsymbol{F}_q[T]\text{中是正规的}$$

$$\Rightarrow g^k \prod_{j=0}^{n-1} \binom{b_j}{2k} \neq 1 \in \boldsymbol{F}_p$$

$$(\text{对于 } 2\leqslant 2k \leqslant b_j \leqslant p-1, 0\leqslant j\leqslant n-1)$$

$$\Rightarrow g^k \prod_{j=0}^{m-1} \binom{b_j}{2k} \neq 1 \in \boldsymbol{F}_p$$

$$(\text{对于 } 2\leqslant 2k \leqslant b_j \leqslant p-1, 0\leqslant j\leqslant m-1)$$

$$\Rightarrow T^2-\frac{d'}{4}\text{ 在 } \boldsymbol{F}_{q'}[T]\text{ 中是正规的.}$$ ▌

以上对于 $p=2$的情形给出了二次正规首1多项式的完全刻划,并且决定了这种多项式的个数(定理4.3.1). 下面讨论 $p\geqslant 3$情形:我们把多项式 $P(T)$和 $P(T+a)$ $(a\in \boldsymbol{F}_q)$称作是等价的,因为它们有同样的正规性.

定理4.3.3 设$3\leqslant p\leqslant 269$, $q=p^\lambda$. 则下面所列是 $\boldsymbol{F}_q[T]$中正规二次首1不可约多项式(等价类)的全部清单(每类中给出形如 $P=T^2-d$的代表元):

(1) $q=3^\lambda$,共 $\varphi(q-1)$类:T^2-d,其中 d 过 $\boldsymbol{F}_q^*$ 的所有(乘法)生成元

(2) $q=5$，　1类：T^2+3

　　$q=25$，　4类：$T^2\pm(1\pm2\sqrt{2})$

(3) $q=7$，　1类：T^2+1

(4) $q=13$，　1类：T^2+5

(5) $q=31$，　2类：T^2+5和 T^2+25

证明　(1) $p=3$时，若 $P=T^2-d$ 正规，由定理4.3.1中的$(2)_3$可知，这等价于 d 是 $\boldsymbol{F}_q^*$ 的生成元(因为$(2)_3$的另一个条件显然满足)，由此即得(1).

利用定理4.3.1中的$(2)_2$，Irland 和 Small 计算出了：当$5\leqslant p\leqslant 269$时，$\boldsymbol{F}_p[T]$中只有以下一些二次正规首1不可约多项式(每类取一个代表)：

$p=5, P=T^2+3$；$p=7, P=T^2+1$；$p=13, P=T^2+5$；$p=31, P=T^2+5$ 和 T^2+25.

根据推论4.3.2，当$5\leqslant p\leqslant 269$并且 $p\neq 5,7,13,31$时，对每个 $q=p^\lambda$，$\boldsymbol{F}_q[T]$中均无二次正规多项式. 所以只需考虑 $q=p^\lambda$，$p=5,7,13,31$和 $\lambda\geqslant 2$的情形.

(2) 设 $p=5, q=p^2$. 取 $\boldsymbol{F}_{25}=\boldsymbol{F}_5(\sqrt{2})$. 若 $T^2-d\in\boldsymbol{F}_{25}[T]$正规，由推论4.3.2的证明可知必然有$(-d)^{\frac{25-1}{5-1}}=3$. 由此得到4个解：$d=\pm1\pm2\sqrt{2}$(另外两个解 $d=\pm\sqrt{2}$ 不是 $\boldsymbol{F}_{25}^*$的生成元). 而定理4.3.1的条件$(2)_3$对于 $q=25$(即 $p=5, \lambda=2$)成立. 所以 $\boldsymbol{F}_{25}[T]$中有4个二次正规首1不可约多项式：$T^2\pm(1\pm2\sqrt{2})$. 对于 $q=125$，我们有

$$3\binom{3}{2}\binom{4}{2}\binom{4}{2}\equiv 1 \pmod 5.$$

即当 $p=5, \lambda=3$时定理4.3.1中的条件$(2)_3$不成立，这表明当 $q=5^3$时，$\boldsymbol{F}_q[T]$中不存在二次正规首1不可约多项式. 由推论4.3.2知，当 $q=5^\lambda(\lambda\geqslant 4)$时也是如此.

对于 $p=7,13,31$，我们分别有：

$$(-4)^2\binom{5}{4}\binom{5}{4}\equiv 1 \pmod 7,$$

$$6\binom{3}{2}\binom{7}{2}\equiv 1 \pmod{13},$$

$$11\cdot\binom{3}{2}\binom{13}{2}\equiv 24\cdot\binom{3}{2}\binom{8}{2}\equiv 1 \pmod{31}.$$

所以当 $q=p^{\lambda}$，$p=7,13,31$和 $\lambda\geqslant 2$时，$\boldsymbol{F}_q[T]$中均不存在二次正规不可约多项式. 这就完成了定理4.3.3的证明. ▌

注记 （1）我们自然提出下列一个初等数论问题：对每个素数 $p\geqslant 37$和 $\boldsymbol{F}_p^*$ 的每个生成元 g，是否一定存在整数 k 和 b，使得

$$2\leqslant 2k\leqslant b\leqslant p-1,\ 2k<p-1,\ g^k\binom{b}{2k}\equiv 1 \pmod{P}\ ?$$

Irland 和 Small 的计算结果表明了当$37\leqslant p\leqslant 269$时，上述问题的答案是肯定的. 如果此问题对所有 $p\geqslant 37$均有肯定的答案，则定理4.3.3就给出了（对所有 q）全部二次正规首1不可约多项式.

（2）如果研究次数$\geqslant 3$的首1不可约多项式的正规性，就需要对 i 的 q-adic 展开式有$\geqslant 3$项的情形给出 $\beta_i(T)$的表达式或素因子分解性质.

这在文献[20]中有一些不完全的结果，可供参阅.

§4.4 指数函数

以上讲述了分圆函数域 $K=k(\Lambda_P)$和 K^+的除子类数 h_P 和 h_P^+ 是否能被域的特征 p 除尽与 Bernoulli-Goss 多项式 $\beta_i(T)$有直接联系. 我们在下节将会看到，理想类数 $h(O_K)^+$是否能被 p 除尽则与 $k=\boldsymbol{F}_q(T)$中一批有理函数（Bernoulli-Carlitz 函数）有直接联系. 这一节是为介绍这批函数作一些准备工作.

我们仍采用符号 $k=\boldsymbol{F}_q(T)$，$R=\boldsymbol{F}_q[T]$. 而 $k_\infty=\boldsymbol{F}_q\left(\left(\frac{1}{T}\right)\right)$ 是 k 对于无限素除子$\infty=\left(\frac{1}{T}\right)$的完备化，$v=v_\infty$是 k_∞中∞-adic 标准指数赋值，$v_\infty\left(\frac{1}{T}\right)=1$. k_∞^{ac}是 k_∞的一个固定的代数闭包. 如前所

述，我们把 k、R、∞、k_∞ 和 k_∞^{ac} 分别看成是数域情形 $\boldsymbol{Q}$、$\boldsymbol{Z}$、通常绝对值、$\boldsymbol{R}$(实数域)和 $\boldsymbol{C}$(复数域)的类比.

对每个 $0\neq\gamma\in k_\infty^{ac}$，$\gamma R$ 是 k_∞^{ac} 中 R-秩为1的格. 对每个正整数 h，定义

$$R(h)=\{A\in R:\deg A<h\}$$

(规定 $\deg(0)=-\infty$)，这是 k 的 h 维 $\boldsymbol{F}_q$-向量子空间，其基可取为 $1,T,T^2,\cdots,T^{h-1}$. 定义

$$e_{\gamma R(h)}(z)=z\prod_{0\neq\alpha\in\gamma R(h)}\left(1-\frac{z}{\alpha}\right). \tag{4.4.1}$$

我们要证明：对每个 $z\in k_\infty^{ac}$ 当 $h\to\infty$ 时，上式右端对于 ∞-adic 拓扑都是收敛的. 于是可定义出 k_∞^{ac} 上的全纯函数：

$$e_{\gamma R}(z)=\lim_{h\to\infty}e_{\gamma R(h)}(z)=z\prod_{0\neq\alpha\in\gamma R}\left(1-\frac{z}{\alpha}\right). \tag{4.4.2}$$

称作关于格 γR 的指数函数. 由于

$$e_{\gamma R}(\gamma z)=\gamma z\prod_{0\neq\alpha\in R}\left(1-\frac{\gamma z}{\gamma\alpha}\right)=\gamma e_R(z), \tag{4.4.3}$$

所以本质上只需研究格 R 上的指数函数：

$$e_R(z)=z\prod_{0\neq\alpha\in R}\left(1-\frac{z}{\alpha}\right),\quad e_{R(h)}(z)=z\prod_{0\neq\alpha\in R(h)}\left(1-\frac{z}{\alpha}\right)$$

即可. 先证明 $e_{R(h)}(z)$ $(h\to\infty)$的收敛性. 显然，$e_{R(h)}(z)$是 $k[z]$中的 q^h 次多项式，它的根集合为 $R(h)$.

定义4.4.1　$f(z)\in k_\infty^{ac}[z]$称作是 *q-线性多项式*，是指它有形式

$$f(z)=\sum_{i=0}^{d}a_iz^{q^i}\quad(a_i\in k_\infty^{ac}).$$

引理4.4.2　设 $f(z)\in k_\infty^{ac}[z]$，则下列两个条件是彼此等价的：

(1) $f(z)$是 q^d 次 q-线性多项式，并且 $f(0)\neq 0$.

(2) $f(z)$在 k_∞^{ac} 中的所有根形式 d 维 $\boldsymbol{F}_q$-向量空间.

证明　(1) $\Rightarrow$ (2)：由于 $f'(z)=f(0)\neq 0$，可知 $f(z)$无重根，易知 $f(z)$的 q^d 个根形成 $\boldsymbol{F}_q$ 上的向量空间.

(2) $\Longrightarrow$ (1)：不妨设 f 是首1多项式. 当 $d=0$时，命题显然成立（此时 $f(z)=z$）. 现设命题对 $d-1$维的情形成立（$d\geqslant 1$），则 k_∞^{ac}的 d 维$\boldsymbol{F}_q$-向量空间可以表示为 $V=V_1\oplus w\boldsymbol{F}_q$，其中$0\neq w\in k_\infty^{ac}$，$V_1$是 $\boldsymbol{F}_q$ 上$d-1$维向量空间. 于是有

$$f(z)=\prod_{\alpha\in V}(z-\alpha)=\prod_{\substack{s\in V_1\\ a\in\boldsymbol{F}_q}}(z-s-aw)$$

$$=\prod_{a\in\boldsymbol{F}_q}g(z-aw)$$

（由归纳假设，$g(z)$ 是 q^{d-1} 次 q-线性多项式）

$$=\prod_{a\in\boldsymbol{F}_q}(g(z)-ag(w))=g(z)^q-g(w)^{q-1}g(z).$$

右端是 q^d 次 q-线性多项式. 由于 $f(z)$有 q^d 个不同的根，因此 $f(z)'=f(0)\neq 0$. ▌

由引理4.4.2可知，对每个 $h\geqslant 0$，$e_{R(h)}(z)$是 $k[z]$中的 q^h 次 q-线性多项式. 现在我们来算这个多项式的系数. 为此，我们引进符号：

$[i]=T^{q^i}-T\quad(i\geqslant 1)$；

$D_0=1,D_i=[i][i-1]^q[i-2]^{q^2}\cdots[1]^{q^{i-1}}=[i]D_{i-1}^q\quad(i\geqslant 1)$；

$L_0=1,L_i=[i][i-1][i-2]\cdots[1]=[i]L_{i-1}\quad(i\geqslant 1)$.

今后仍用 R_1表示 $R=\boldsymbol{F}_q[T]$中首1多项式的全体.

引理4.4.3 (1) 对于上面定义的 $\boldsymbol{F}_q[T]$的中多项式，有

$$[i]=\prod_{\substack{P\\ \deg P\mid i}}P,\quad D_h=\prod_{\substack{A\in R_1\\ \deg A=h}}A,\quad L_h=\mathrm{LCM}\{A\in R_1:\deg A=h\},$$

上式中 P 表示 R 中的首1不可约多项式，LCM 表示首1多项式的最小公倍式.

(2) 对每个 $h\geqslant 0$，有

$$e_{R(h)}(z)=\sum_{i=0}^{h}(-1)^i\frac{L_h}{D_iL_{h-i}^{q^i}}z^{q^i}.$$

证明 (1) 熟知$[i]=T^{q^i}-T$ 恰好是 $\boldsymbol{F}_q[T]$中的次数能除尽 i 的所有首1不可约多项式的积. 另一方面，对于每个首1不可约多项

式 P，以 v_P 表示 k 的 P-adic 标准指数赋值，$v_P(P)=1$，则不难算出

$$v_P(D_h)=\sum_{i=1}^{[h/\deg P]} q^{h-i\deg P}=v_P\left(\prod_{\substack{A\in R_1\\ \deg A=h}} A\right),$$

$$v_P(L_h)=\left[\frac{h}{\deg P}\right]=v_P(\mathrm{LCM}\{A\in R_1;\deg A=h\}).$$

由此即得关于 D_h 和 L_h 的表达式.

(2) 我们先证明：对每个 $h\geqslant 0$，有

$$\prod_{a\in R(h)}(z-a)=\sum_{i=0}^{h}(-1)^{h-i}\frac{D_h}{D_i L_{h-i}^{q^i}}z^{q^i}, \qquad (4.4.4)$$

当 $h=0$时，(4.4.4)式两端均为 z. 现设(4.4.4)式对于 h 成立，并记(4.4.4)式左端为 $\tilde{e}_h(z)$，则

$$\tilde{e}_{h+1}(z)=\prod_{a\in R(h+1)}(z-a)=\tilde{e}_h(z)\cdot\prod_{a\in F_q^*}\prod_{B\in R(h)}(z-aT^h-B)$$

$$=\tilde{e}_h(z)\prod_{a\in F_q^*}\tilde{e}_h(z-aT^h)$$

$$=\tilde{e}_h(z)\prod_{a\in F_q^*}(\tilde{e}_h(z)-a\tilde{e}_h(T^h))$$

（由于 $\tilde{e}_h(z)$ 是 q-线性多项式）

$$=\tilde{e}_h(z)\prod_{a\in F_q^*}(\tilde{e}_h(z)-aD_h)$$

（由本引理的(1)）

$$=\tilde{e}_h(z)^q-\tilde{e}_h(z)D_h^{q-1}$$

$$=\sum_{i=0}^{h}(-1)^{h-i}\left(\frac{D_h}{D_i L_{h-i}^{q^i}}\right)^q z^{q^{i+1}}$$

$$-D_h^{q-1}\sum_{i=0}^{h}(-1)^{h-i}\frac{D_h}{D_i L_{h-i}^{q^i}}z^{q^i}$$

（由归纳假设）

$$=z^{q^{h+1}}+(-1)^{h+1}\frac{D_h^q}{L_h}z$$

$$+\sum_{i=1}^{h}(-1)^{h+1-i}z^{q^i}\left(\frac{D_h^q}{D_iL_{h-i}^{q^i}}+\frac{D_h^q}{D_{i-1}^qL_{h-i+1}^{q^i}}\right)$$

$$=\sum_{i=0}^{h+1}\frac{D_{h+1}}{D_iL_{h+1-i}^{q^i}}(-1)^{h+1-i}z^{q^i}.$$

这就证明了(4.4.4)式.特别地,我们有

$$\prod_{0\neq a\in R(h)}a=\left.\frac{\tilde{e}_h(z)}{z}\right|_{z=0}=(-1)^h\frac{D_h}{L_h}.$$

再由(4.4.4)式即知

$$e_{R(h)}(z)=\left(\prod_{0\neq a\in R(h)}a\right)^{-1}\tilde{e}_h(z)=\sum_{i=0}^{h}(-1)^i\frac{L_h}{D_iL_{h-i}^{q^i}}z^{q^i}.$$ ▌

现在对每个 $h\geqslant 2$,令

$$\pi_h=\prod_{i=1}^{h-1}\left(1-\frac{[i]}{[i+1]}\right), \tag{4.4.5}$$

由于 $v\left(\frac{[i]}{[i+1]}\right)=\deg[i+1]-\deg[i]=q^{i+1}-q^i\to\infty$ (当 $i\to\infty$ 时),所以无穷乘积

$$\pi=\lim_{h\to\infty}\pi_h=\prod_{i=1}^{\infty}\left(1-\frac{[i]}{[i+1]}\right)$$

收敛于 k_∞ 中.我们用 $\tilde{\pi}$ 表示方程 $Y^{q-1}=-[1]\pi^{q-1}$ 在 k_∞^{ac} 中的一个根(全部根为 $\alpha\tilde{\pi}(\alpha\in F_q^*)$),则格 $\tilde{\pi}R$ 与根 $\tilde{\pi}$ 的选取方式无关.对于这个格,指数函数有更简单的展开式,以下令

$$e(z)=e_{\tilde{\pi}R}(z). \tag{4.4.6}$$

定理4.4.4 (1) $e(z)=\sum_{i\geqslant 0}\frac{z^{q^i}}{D_i}$, $e(Tz)=Te(z)+e(z)^q$.

(2) 令

$$\log(z)=\sum_{i\geqslant 0}(-1)^i\frac{z^{q^i}}{L_i},$$

则对每个 $z\in k_\infty^{ac}$,$v(z)>-1$, 均有:

$$\log(e(z))=z,\ e(\log(z))=z.$$

证明 (1) 引理4.4.3给出了 $e_{R(h)}(z)$ 的公式.现在计算它的极限 $e_R(z)=\lim_{h\to\infty}e_{R(h)}(z)$.通过计算,由(4.4.5)式可知引理4.4.3

的(2)可表示成(令 $\pi_1=\pi_0=1$)：

$$e_{R(h)}(z)=\frac{1}{\pi_h}\sum_{i=0}^{h}(-1)^i\frac{z^{q^i}}{D_i}[1]^{\frac{q^i-1}{q-1}}\pi_{h-i}^{q^i}. \qquad (4.4.7)$$

现在记

$$\begin{aligned}\sigma_h &= \sum_{i=0}^{h}(-1)^i\frac{z^{q^i}}{D_i}[1]^{\frac{q^i-1}{q-1}}(\pi_{h-i}-\pi)^{q^i}\\ &=\sigma_{h,1}+\sigma_{h,2}, \end{aligned}\qquad (4.4.8)$$

其中

$$\sigma_{h,1}=\sum_{0\leqslant i\leqslant\left[\frac{h}{2}\right]},\sigma_{h,2}=\sum_{\left[\frac{h}{2}\right]\leqslant i\leqslant h}.$$

现在证明当 $h\to\infty$ 时，$\sigma_h\to 0$. 首先，由 $\pi_{i+1}-\pi_i=-\frac{[i-1]}{[i]}\pi_i$ 和 $v(\pi_i)=0$ 可知

$$v(\pi_{i+1}-\pi_i)=v\left(\frac{[i-1]}{[i]}\right)=q^i-q^{i-1}\quad(i\geqslant 2).$$

于是对每个 $i,j\geqslant 2$，有

$$v(\pi_{i+j}-\pi_i)=\min_{1\leqslant\lambda\leqslant j}\{v(\pi_{i+\lambda}-\pi_{i+\lambda-1})\}=q^i-q^{i-1}\quad(i\geqslant 2).$$

令 $j\to\infty$，即知 $v(\pi-\pi_i)=q^i-q^{i-1}\ (i\geqslant 2)$，所以

$$\begin{aligned}&v\left(\frac{z^{q^i}}{D_i}[1]^{\frac{q^i-1}{q-1}}(\pi_{h-i}-\pi)^{q^i}\right)\\ &=(v(z)+i)q^i-\frac{q(q^i-1)}{q-1}+q^h-q^{h-1}\quad(i\leqslant h-2).\end{aligned}$$

由此可知当 $h\to\infty$ 时，$\sigma_{h,1}\to 0$. 另一方面，$\sigma_{h,2}$ 的和式中的每项(包括 $i=h-1$ 和 h)均趋于零. 故当 $h\to\infty$ 时，$\sigma_{h,2}\to 0$. 这就证明了 $\sigma_h\to 0$. 现在在公式(4.4.7)中令 $h\to\infty$，得到

$$\begin{aligned}e_R(z)&=\frac{1}{\pi}\sum_{i\geqslant 0}(-1)^i\frac{z^{q^i}}{D_i}[1]^{\frac{q^i-1}{q-1}}\pi^{q^i}\\ &=\frac{1}{\tilde{\pi}}\sum_{i\geqslant 0}(\tilde{\pi}z)^{q^i}/D_i\end{aligned}$$

$$\left(注意(-1)^i=(-1)^{\frac{q^i-1}{q-1}}\right).$$

再由(4.4.3)式即知

$$e(z)=e_{\tilde{\pi}R}(z)=e_R(\tilde{\pi}^{-1}z)\tilde{\pi}=\sum_{i\geqslant 0}\frac{z^{q^i}}{D_i},$$

进而由此式可知

$$\begin{aligned}Te(z)+e(z)^q&=\sum_{i\geqslant 0}\left(\frac{Tz^{q^i}}{D_i}+\frac{z^{q^{i+1}}}{D_i^q}\right)\\&=Tz+\sum_{i\geqslant 1}z^{q^i}\left(\frac{T}{D_i}+\frac{1}{D_{i-1}^q}\right)\\&=\sum_{i\geqslant 0}\frac{(Tz)^{q^i}}{D_i}=e(Tz).\end{aligned}$$

(2) 利用∞-adic 估计，可知级数 $\log(z)$ 在 $v(z)>-1$ 时是收敛的，并且此时 $v(e(z))>-1$，所以当 $v(z)>-1$ 时，$e(\log(z))$ 和 $\log(e(z))$ 均有意义. 为了证明(2)中的两个等式，只需把级数 $e(z)$ 和 $\log(z)$ 均看成是"形式"幂级数即可. 换句话说，我们考虑集合

$$B=\{\sum_{i\geqslant 0}a_iz^{q^i};a_i\in k_\infty^{ac}\}.$$

引入运算：对于 $\alpha=\sum_{i\geqslant 0}a_iz^{q^i}$，$\beta=\sum_{i\geqslant 0}b_iz^{q^i}$，令

$$\alpha+\beta=\sum_{i\geqslant 0}(a_i+b_i)z^{q^i},\ \alpha\circ\beta=\sum_{i\geqslant 0}a_i\beta^{q^i}=\sum_{i,j\geqslant 0}a_ib_j^{q^i}z^{q^{i+j}},$$

即 $(\alpha\circ\beta)(z)=\alpha(\beta(z))$. 则 B 对这两种运算是非交换环，幺元素为 z. 并且易知：元素 $\alpha=\sum_{i\geqslant 0}a_iz^{q^i}$ 对于乘法 ∘ 可逆的充要条件为 $a_0\neq 0$. 于是 $e(z)$ 为 B 中的可逆元素，记它的逆为 $\log(z)$. 由于 $e(Tz)=Te(z)+e(z)^q$，将 z 改用 $\log(z)$，得 $e(T\log z)=Tz+z^q$. 两端取 log，得到

$$T\log(z)=\log(Tz)+\log(z^q).$$

令 $\log(z)=\sum_{i\geqslant 0}a_iz^{q^i}$，则 $Ta_i=a_iT^{q^i}+a_{i-1}\ (i\geqslant 1)$，而 $a_0=\log(z)|_{z=0}=e(z)^{-1}|_{z=0}=1$. 于是 $a_i=-a_{i-1}[i]^{-1}(i\geqslant 1)$. 递推得到 $a_i=(-1)L_i^{-1}(i\geqslant 0)$. 这就证明了 $\log(z)=\sum_{i\geqslant 0}(-1)^i\frac{z^{q^i}}{L_i}$. ∎

注记4.4.5 (1) 我们说过，$R=F_q[T]$ 和 k_∞^{ac} 分别是 Z 和 C 的

类比. 由于

$$\sin x = \pi x \prod_{0 \neq n \in \mathbf{Z}} \left(1 - \frac{x}{n}\right) = \pi x \prod_{n \geq 1} \left(1 - \frac{x^2}{n^2}\right) \quad (\pi = 3.14159\cdots),$$

$$e_R(z) = z \prod_{0 \neq \alpha \in R} \left(1 - \frac{z}{\alpha}\right) = z \prod_{\alpha \in R_1} \left(1 - \left(\frac{z}{\alpha}\right)^{q-1}\right),$$

所以指数函数 $e_R(z)$ 可以看成是正弦函数 $\sin x$ 的类比. $\sin \pi x$ 的零点集合是 C 中的秩为1的格 $\mathbf{Z}$，而 $e_R(z)$ 的零点集合是 k_∞^{ac} 中秩为1的格 R. 另一方面，函数 $e(z) = e_{\tilde{\pi} R}(z)$ 的周期为 $\tilde{\pi} R$ （即对每个 $a \in \tilde{\pi} R$，$e(z+a) = e(z)$），所以它又像是周期为 $2\pi\sqrt{-1}\mathbf{Z}$ 的指数函数 e^z. 我们知道 $\pi = 3.14159\cdots$ 在 Q 上是超越的. 类似地，Carlitz 的一个学生 Wade 在40年代证明了 $\tilde{\pi}$ 为 $k = F_q(T)$ 上的超越元素.

(2) 现在说明指数函数

$$e(z) = e_{\tilde{\pi} R}(z) = z \prod_{0 \neq \alpha \in \tilde{\pi} R} \left(1 - \frac{z}{\alpha}\right)$$

和 § 4.1中定义的 Goss zeta 函数

$$\zeta_\infty(s) = \sum_{A \in R_1} A^{-s} \quad (s \in \mathbf{Z})$$

之间的联系. 由于 $e(z)$ 的微商为 $e'(z) = 1$，得到

$$\frac{1}{e(z)} = \frac{e'(z)}{e(z)} = \sum_{\alpha \in \tilde{\pi} R} \frac{1}{z - \alpha},$$

于是

$$\begin{aligned} \frac{z}{e(z)} &= 1 + \sum_{0 \neq \alpha \in \tilde{\pi} R} \frac{z}{z - \alpha} = 1 - \sum_{0 \neq \alpha \in \tilde{\pi} R} \sum_{i \geq 1} \left(\frac{z}{\alpha}\right)^i \\ &= 1 - \sum_{i \geq 1} z^i \sum_{0 \neq \alpha \in \tilde{\pi} R} \alpha^{-i} = 1 - \sum_{i \geq 1} \left(\frac{z}{\tilde{\pi}}\right)^i \sum_{0 \neq A \in R} A^{-i}. \end{aligned}$$

当 $(q-1) \nmid i$ 时，

$$\sum_{0 \neq A \in R} A^{-i} = \sum_{A \in R_1} A^{-i} \sum_{a \in F_q^*} a^{-i} = 0;$$

而当 $(q-1) \mid i$ 时，

$$\sum_{0 \neq A \in R} A^{-i} = (q-1) \sum_{A \in R_1} A^{-i} = -\sum_{A \in R_1} A^{-i} = -\zeta_\infty(i).$$

于是

$$\frac{z}{e(z)}=\sum_{i\geqslant 0}\left(\frac{z}{\tilde{\pi}}\right)^{i(q-1)}\zeta_{\infty}(i(q-1)). \qquad (4.4.9)$$

但是 $e(z)=\sum_{i\geqslant 0} z^{q^i}/D_i$ 的系数属于 k，所以 $z/e(z)$ 的系数 $\zeta_{\infty}(i(q-1))/(\tilde{\pi})^{i(q-1)}$ $(i\geqslant 0)$也属于 k. 由于 $\tilde{\pi}$ 在 k 上是超越的，所以$\zeta_{\infty}(i(q-1))$ $(i\geqslant 1)$在 k 上均是超越的. 已知整数环 $\boldsymbol{Z}$ 的单位群是2阶循环群$\{\pm 1\}$，而环 $R=\boldsymbol{F}_q[T]$的单位群是 $q-1$阶循环群 $\boldsymbol{F}_q^*$，所以函数域中的 $q-1$相当于数域情形的2(又例如说：$[\boldsymbol{Q}(\zeta_m):\boldsymbol{Q}(\zeta_m)^+]=2$，$[k(\Lambda_M):k(\Lambda_M)^+]=q-1$)，所以$(q-1)\boldsymbol{Z}$ 相当于偶数集合$2\boldsymbol{Z}$. 对于黎曼 zeta 函数 $\zeta(s)=\sum_{n\geqslant 1} n^{-s}$，熟知 $\zeta(2n)/\pi^{2n}\in\boldsymbol{Q}$(对每个正整数 n). 因此上述结果 $\zeta_{\infty}(i(q-1))/\tilde{\pi}^{i(q-1)}\in k(i\geqslant 1)$可以看成是它的模拟.

§4.5 Bernoulli-Carlitz"数"和理想类数

在多项式环 $\boldsymbol{F}_q[T]$中什么是阶乘函数 $n!$的模拟?这是 Carlitz 在30年代考虑的一个问题. 设 $m=a_0+a_1q+\cdots+a_vq^v$ 是非负整数 m 的 q-adic 展开. 定义 $\boldsymbol{F}_q[T]$中的多项式

$$\Gamma_m=D_0^{a_0}D_1^{a_1}\cdots D_r^{a_r}, \qquad (4.5.1)$$

其中 D_i 的定义见§4.4. 我们知道，$n!$有素因子分解式：

$$n=\prod_p p^{a_p},\quad a_p=\sum_{e\geqslant 1}\left[\frac{n}{p^e}\right].$$

下面的引理表明 Γ_m 在 $R=\boldsymbol{F}_q(T)$中有类似的分解式.

引理4.5.1 $\Gamma_0=1$. 对于 $m\geqslant 1$，

$$\Gamma_m=\prod_P P^{a_P},\quad a_P=\sum_{e\geqslant 1}\left[\frac{m}{q^{e\deg P}}\right],$$

其中 P 过 $\boldsymbol{F}_q[T]$中的首1不可约多项式.

证明 以 v_P 表示 $k=\boldsymbol{F}_q(T)$中 P-adic 标准指数赋值，$v_P(P)=1$，对于 $m=a_0+a_1q+\cdots+a_rq^r$，我们有

$$\begin{aligned}
a_P &= v_P(\Gamma_m) = \sum_{i=1}^{r} a_i v_P(D_i) \\
&= \sum_{i=1}^{r} a_i \sum_{e=1}^{i} v_P\left(T^{q^i} - T^{q^{i-e}}\right) = \sum_{e\geqslant 1} v_P\left(T^{q^e} - T\right) \sum_{i=e}^{r} a_i q^{i-e} \\
&= \sum_{e\geqslant 1} \left[\frac{m}{q^e}\right] v_P\left(T^{q^e} - T\right) = \sum_{\substack{e\geqslant 1 \\ \deg P | e}} \left[\frac{m}{q^e}\right] \\
&= \sum_{e\geqslant 1} \left[\frac{m}{q^{e\deg P}}\right]. \quad \blacksquare
\end{aligned}$$

定义 设 $e(z)=e_{\bar{\pi}R}(z)$是§4.4中定义的指数函数.令

$$\frac{z}{e(z)} = \sum_{m\geqslant 0} \frac{B_m}{\Gamma_m} z^m,$$

其中 $B_m(m\geqslant 0)$称为 Bernoulli-Carlitz 数(实际上它们是 $k=\boldsymbol{F}_q(T)$中的有理函数). Carlitz 把 B_m 作为通常 Bernoulli 数 b_m 的类比,因为对于 b_m,有公式

$$\frac{z}{e^z - 1} = \sum_{m\geqslant 0} \frac{b_m}{m!} z^m.$$

由(4.4.9)式可以看出 B_m 和 $\zeta_\infty(s)$之间的联系:对于 $m\geqslant 0$,

$$B_m = \begin{cases} \Gamma_m \zeta_\infty(m)/\tilde{\pi}^m, & \text{若}(q-1)|m, \\ 0, & \text{否则}. \end{cases}$$

其中对于$(q-1)|m\geqslant 0$,有

$$\zeta_\infty(m) = \sum_{A\in R_1} A^{-m} = -\sum_{A\in R} A^{-m}.$$

进而,定理4.4.4表明了指数函数的反函数为

$$\log(z) = \sum_{h\geqslant 0} (-1)^h \frac{z^{q^h}}{L_h},$$

由此可知

$$\frac{z}{e(z)} = \sum_{h\geqslant 0} (-1)^h \frac{e(z)^{q^h - 1}}{L_h},$$

记
$$e(z)^{q^h-1} = \sum_{m\geqslant 0} \frac{A_m^{(h)}}{\Gamma_m} z^m,$$

则有
$$B_m = \sum_{q^h \leqslant m+1} (-1)^h \frac{A_m^{(h)}}{L_h}. \tag{4.5.2}$$
通常的 Bernoulli 数 b_m 是有理数，它的部分分式展开式有：

von Staudt 定理 $b_m = -\sum_{(p-1)|m} \frac{1}{p} \pmod{\mathbf{Z}}$.

Carlitz 对于有理函数 B_m 给出了类似的部分分式展开，近来 D. Goss对此作了更系统的处理. 为此目的，我们引入如下定义：

定义 对于 $R=\boldsymbol{F}_q[T]$中的元素构成的序列$\{A_0,A_1,\cdots,A_n,\cdots\}$，形式幂级数$\sum\limits_{m\geqslant 0}\frac{A_m}{\Gamma_m}z^m$ 称作 Hurwitz 级数，简称 H-级数.

例如：指数函数 $e(z)=\sum\limits_{h\geqslant 0} z^{q^h}/D_h$ 是 H-级数，因为当 $m=q^h$ 时，$\Gamma_{q^h}=D_h$，所以 $A_m=1$，而 $m\neq q^h$ 时，$A_m=0$.

定理4.5.2 (1) 所有 H-级数对于通常形式的幂级数的代数运算形成 R-交换代数，并且 H-级数$\sum\limits_{m\geqslant 0}\frac{A_m}{\Gamma_m}z^m$ 可逆时（即 $A_0\neq 0$ 时），则其逆为 H-级数当且仅当 $A_0\in \boldsymbol{F}_q^*$.

(2) 若 $s=\sum\limits_{m\geqslant 0}\frac{A_m}{\Gamma_m}z^m$ 是 H-级数，并且 $A_0=0$，则对每个 $h\geqslant 0$，s^h/Γ_h 为 H-级数. 所以对每个 H-级数 s_1，$s_1(s(z))$也是 H-级数.

证明 (1) 设 $\alpha=\sum\frac{A_m}{\Gamma_m}z^m$ 和 $\beta=\sum\frac{B_m}{\Gamma_m}z^m$ 均是 H-级数，则 $\alpha+\beta$ 显然是 H-级数，并且对于 $A\in R$，$A\alpha$ 也是 H-级数. 再证 $\alpha\beta=\sum\frac{C_m}{\Gamma_m}z^m$ 也是 H-级数，其中
$$C_m = \sum_{i+j=m} \frac{\Gamma_m}{\Gamma_i\Gamma_j}A_iB_j.$$
这只需证明：当 $i+j=m$，$i,j\geqslant 0$时，$\Gamma_i\Gamma_j \mid \Gamma_m$. 这一点由引理4.5.1可直接看出. 这就证明了所有 H-级数形成了 R-交换代数. 进而若 $\alpha\beta=1$，则 $A_0B_0=1$，于是 $A_0\in\boldsymbol{F}_q^*$. 反之，若 $A_0\in\boldsymbol{F}_q^*$，则 $B_0=A_0^{-1}$，而当 $m\geqslant 1$时，可递推出来
$$B_m = -A_0^{-1}\Bigg(\sum_{\substack{j=0\\ i+j=m}}^{m-1}\frac{\Gamma_m}{\Gamma_i\Gamma_j}A_iB_j\Bigg)\in R.$$

所以 $\alpha^{-1}=\beta$ 是 H-级数.

(2) 设 $s=\sum_{m\geqslant 1}\frac{A_m}{\Gamma_m}z^m$ 是 H-级数,即 $A_m\in R(m\geqslant 1)$. 对于 $h=\sum_i c_i q^i$,我们有

$$S^h/\Gamma_h=\prod_i s^{c_i q^i}/\Gamma_{q^i}^{c_i}.$$

所以只需对 $h=q^i$ 情形证明 s^h/Γ_h 是 H-级数即可. 这时有

$$s^h/\Gamma_h=\sum_{m\geqslant 1}\frac{A_m^{q^i}}{\Gamma_{mq^i}}z^{mq^i}\cdot\frac{\Gamma_{mq^i}}{\Gamma_m^{q^i}\Gamma_{q^i}}.$$

所以只需证明 $\Gamma_m^{q^i}\Gamma_{q^i}\mid\Gamma_{mq^i}$. 设 $m=a_0+a_1q+\cdots+a_rq^r$,则

$$\Gamma_{qm}/\Gamma_m^q=\prod_{j=0}^r(D_{j+1}^{a_j}/D_j^{a_jq})=\prod_{j=0}^r[j+1]^{a_j},$$

$$\Gamma_{q^2m}/\Gamma_m^{q^2}=(\Gamma_{qm}/\Gamma_m^q)^q(\Gamma_{q^2m}/\Gamma_{qm}^q)=\prod_{j=0}^r([j+2][j+1]^q)^{a_j}.$$

由此可递归得出:

$$\Gamma_{q^im}/\Gamma_m^{q^i}=\prod_{j=0}^r([j+i][j+i-1]^q\cdots[j+1]^{q^{i-1}})^{a_j}$$

$$=\prod_{j=0}^r\left(\frac{D_{i+j}}{D_j^{q^i}}\right)^{a_j}.\tag{4.5.3}$$

现在记 $(i,j)=D_{i+j}/D_iD_j^{q^i}$,则 $(0,j)=(i,0)=1$. 而当 $i\geqslant 1$ 时,

$$(i,j)=[i+j]D_{i+j-1}^q/D_iD_j^{q^i}=([i]+[j]^{q^i})D_{i+j-1}^q/D_iD_j^{q^i}$$

$$=(i-1,j)^q+\left(\frac{D_{i+j-1}}{D_{j-1}^{q^i}}\right)^{q-1}(i,j-1).$$

由此可归纳得出:对任意 i、$j\geqslant 0$,均有 $(i,j)\in R$. 由(4.5.3)式表明了 $D_i=\Gamma_{q^i}$ 除尽 $\Gamma_{q^im}/\Gamma_m^{q^i}$,即 $\Gamma_m^{q^i}\Gamma_{q^i}\mid\Gamma_{mq^i}$. ▌

定理4.5.3　设 $m\geqslant 0$, $B_m=\frac{N_m}{W_m}$,其中 N_m 和 W_m 是 $F_q[T]$ 中互素的多项式. 则 W_m 没有重因子,并且若 P 是 W_m 的首1不可约因子,则 $q^{\deg P}-1\mid m$.

证明　定理4.5.2表明了 $e(z)^{q^h-1}=\sum_{m\geqslant 0}\frac{A_m^{(h)}}{\Gamma_m}z^m$ 是 H-级数,即

$A_m^{(h)}\in R$，又因 $e(z)^{q^h-1}/\Gamma_{q^h-1}$ 也是 H-级数，于是 $\Gamma_{q^h-1}\mid A_m^{(h)}$. 注意 $\Gamma_{q^h-1}=(D_1\cdots D_{h-1})^{q-1}$，可知

$$A_m^{(h)}/L_h=\frac{A_m^{(h)}}{\Gamma_{q^h-1}}\cdot\frac{(D_1\cdots D_{h-1})^{q-1}}{L_{h-1}}\cdot\frac{1}{[h]}\in\frac{1}{[h]}R.$$

再由(4.5.2)式便知 W_m 的因子都是 $\mathrm{LCM}\{[h]:q^h\leqslant m+1\}$ 的因子，由于每个$[h]$都没有重因子，所以 W_m 也是如此.

设 P 是 W_m 的首1不可约因子，$r=\deg P$. 现在要证明 $(q^r-1)\mid m$. 定理4.4.4表明

$$e(Tz)=e(z)^q+Te(z)=\rho_T(e(z)),$$

其中 ρ_T 是§1.1节所述的 Carlitz 模作用. 于是对每个 $A\in R, A\neq 0$，有

$$e(Az)=\rho_A(e(z))=\sum_{i=0}^{\deg A}\begin{bmatrix}A\\ i\end{bmatrix}e(z)^{q^i}\quad(\text{引理 }1.1.1),$$

其中$\begin{bmatrix}A\\ 0\end{bmatrix}=A$. 于是

$$A\left(\frac{Az}{e(Az)}-\frac{z}{e(z)}\right)=-\frac{z\sum_{i=1}^{\deg A}\begin{bmatrix}A\\ i\end{bmatrix}e(z)^{q^i-1}}{1+A^{-1}\sum_{i=1}^{\deg A}\begin{bmatrix}A\\ i\end{bmatrix}e(z)^{q^i-1}}.$$

由于右端是 H-级数(定理4.5.2)，所以左端

$$A\left(\frac{Az}{e(Az)}-\frac{z}{e(z)}\right)=\sum_{m\geqslant 0}\frac{B_m}{\Gamma_m}A(A^m-1)z^m$$

也是 H-级数. 这表明了 $P\mid W_m\mid A(A^m-1)$. 现在取 A 为 q^r-1阶循环群$(R/(P))^*$的生成元代表，则 $P\mid A^m-1$，于是 $q^r-1\mid m$. ∎

这个定理表明 B_m 有如下形式的部分分式展开式：

$$B_m=\sum_{q^{\deg P}-1\mid m}\frac{a_P}{P}+g_m,$$

其中 $g_m, a_P\in R$，$\deg a_P<\deg P$. 这和通常 Bernoulli 数的部分分式展开(von Staudt 定理)有相似的形式. 经过详细计算，D. Goss[21] 得到如下的确切结果. 证明从略.

定理4.5.4　(1) 设 $q\neq 2, q=p^n$. 令 $m=\sum_{i=0}^{r}\beta_i p^i$ 是 m 的 P-adic展开. 如果 m 满足以下两个条件:

① $(p-1)n\mid\sum\beta_i$ (令 $h=\sum\beta_i/n(p-1)$);

② $(q^h-1)\mid m$.

则

$$B_m=g_m-\frac{(-1)^x}{y}\sum_{\deg P=h}\frac{1}{P},$$

其中 $g_m\in R=\boldsymbol{F}_q[T]$, $x\geqslant 0$ 和 $y\in\boldsymbol{F}_q^*$ 按下面方式决定: 设 $m=\sum_{j=0}^{s}\alpha_j q^{hj}$ 为 q^h-adic 展开, 则

$$x=h(\alpha_1+2\alpha_2+\cdots+s\alpha_s)+nh,\quad y=\prod_{i=0}^{r}(\beta_i!).$$

如果 m 不同时满足①和②, 则 $B_m\in\boldsymbol{F}_q[T]$.

(2) 设 $q=2$, 如果 m 满足上述条件①和②, 则

当 $h\neq 2$时, $B_m=g_m+\sum_{\deg P=h}\frac{1}{P}$, $g_m\in\boldsymbol{F}_2[T]$.

当 $h=2$, $2\mid m$ 时, $B_m=g_m+\frac{1}{T^2+T+1}$, $g_m\in\boldsymbol{F}_2[T]$.

当 $h=2$, $2\nmid m$ 时, $B_m=g_m+\frac{1}{T}+\frac{1}{T+1}+\frac{1}{T^2+T+1}$,

$$g_m\in\boldsymbol{F}_2[T].$$

若 m 不同时满足条件①和②, 则

当$2\mid m$ 时, $B_m\in\boldsymbol{F}_2[T]$.

当$2\nmid m$ 时, $B_m=g_m+\frac{1}{T}+\frac{1}{T+1}$, $g_m\in\boldsymbol{F}_2[T]$.

最后我们介绍 Bernoulli-Carlitz 数 B_m 和分圆函数域 $k(\Lambda_P)^+$ 理想类数的关系.

定理4.5.5[40]　设 $k=\boldsymbol{F}_q(T)$, $q=p^n$, P 为 $\boldsymbol{F}_q[T]$中首1不可约多项式, $d=\deg P\geqslant 1$, $K=k(\Lambda_P)$. 如果 $p\mid h(O_K)^+$, 则存在某个 m, $1\leqslant m\leqslant q^d-2$, $(q-1)\mid m$, 使得 $v_p(B_m)\geqslant 1$, 即 P 能除尽 B_m 的分子.

证明 设 λ 是一个本原 P-torsion 元素,则 $\mathscr{P}=(\lambda)$是 O_K 的素理想(完全分歧). 以 $K_{\mathscr{P}}$ 表示 K 对 $\mathscr{P}$ 的局部化,则 $K_{\mathscr{P}}\cong \boldsymbol{F}_q((\lambda))$,所以对 $K_{\mathscr{P}}$ 中每个元素 α, $v_{\mathscr{P}}(\alpha)=0$,有 $f(u)\in \boldsymbol{F}_q[[u]]$,使得 $f(0)\in \boldsymbol{F}_q^*$, $\alpha=f(\lambda)$. 由于 $f'(e(z))$和 $f(e(z))^{-1}$都是 H-级数(定理4.5.2),所以

$$\frac{f'(e(z))}{f(e(z))}=\sum_{i\geqslant 0}\frac{A_i}{\Gamma_i}z^i$$

也是 H-级数,即 $A_i\in R$(对每个 $i\geqslant 0$). 现在对每个 i, $1\leqslant i\leqslant q^d-2$,定义映射:

$$\varphi_i: U_K\to R/(P),\alpha\mapsto A_{i-1}\pmod P.$$

先说明这个映射的可定义性,即与 $f(u)$的选取方式无关. 如果 $g(u)\in \boldsymbol{F}_q[[u]]$, $g(\lambda)=\alpha$,则 $f(u)-g(u)$被 λ 的极小多项式

$$\rho_P(u)/u=\prod_{0\neq A\in R/(P)}(u-\lambda^A)$$

除尽,即

$$f(u)=g(u)+\rho_P(u)u^{-1}h(u),\ h(u)\in \boldsymbol{F}_q[[u]].$$

令 $$\frac{g'(e(z))}{g(e(z))}=\sum_{i\geqslant 0}\frac{B_i}{\Gamma_i}z^i,\ B_i\in \boldsymbol{F}_q[T].$$

由 $\rho_P(u)\equiv 0\pmod{P,u^{q^d}}$可知

$$\rho_P(e(z))e(z)^{-1}\equiv 0\pmod{P,z^{q^d-1}},$$

$$\frac{d}{dz}(\rho_P(e(z))e(z)^{-1})\equiv 0\pmod{P,z^{q^d-2}}.$$

由此可知 $A_i\equiv B_i\pmod P$,即映射 $\varphi_i(1\leqslant i\leqslant q^d-2)$均是可定义的. 进而由$(fg)'/fg=f'/f+g'/g$ 可知 φ_i 是群的同态. 记 $U_K=\boldsymbol{F}_q^*\times U$,其中 U 是自由阿贝尔群,不妨设 U 包含由$\{\lambda^A/\lambda: 1\neq A\in R_1,\deg A<d\}$生成的分圆单位群 $C=C_y(K^+)$(其定义见第2章). 于是有

$$[U:C]=[U_K:\boldsymbol{F}_q^*C]=[U_K^+:\boldsymbol{F}_q^*C]\ (\text{引理 } 1.2.6)$$
$$=h(O_K)^+\quad(\text{定理 } 2.1.1).$$

由 $\boldsymbol{F}_q^*\subseteq\ker(\varphi_i)$给出同态

$$\varphi_i : U \to R/(P),$$

再由 $R/(P)$ 的特征为 p 诱导出同态：

$$\varphi_i : U/U^p \to R/(P) \quad (1 \leqslant i \leqslant q^d - 2).$$

以 $\hat{G}$ 表示伽罗华群

$$G = \mathrm{Gal}(K/k) \cong (R/(P))^* \cong F_{q^d}^*$$

的特征群. 对每个 $\chi \in \hat{G}$，以 $U(\chi)$ 表示 $U/U^p \otimes_{F_p} F_{q^d}$ 的 χ-分支. 类似地有 $C(\chi)$，则 $C(\chi)$ 是 $U(\chi)$ 的子群，并且当 $\chi \neq \chi_0$ 时，$C(\chi)$ 是由 $\lambda^{\varepsilon_\chi}$ 生成的，其中 $\varepsilon_\chi = \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}$. 而当 $\chi = \chi_0$ 时，$C(\chi) = U(\chi) = (1)$. 由于 $U_K = F_q^* U_K^+$，可知当 χ 是非实特征时，也有 $U(\chi) = C(\chi) = (1)$. 所以

$$U/C = \bigoplus_{\chi_0 \neq \chi \in \hat{G}^+} U(\chi)/C(\chi).$$

如果 $p \mid h(O_K)^+ = [U : C] = \prod_{\chi_0 \neq \chi \in \hat{G}^+} [U(\chi) : C(\chi)]$，

则存在 $\chi_0 \neq \chi \in \hat{G}^+$，使得 $p \mid [U(\chi) : C(\chi)]$. 由于 $\dim_{F_{q^d}} U(\chi) = 1$，可知 $C(\chi) \subseteq U^p$. 于是

$$\varphi_i(\lambda^{\varepsilon_\chi}) = 0, 1 \leqslant i \leqslant q^d - 2. \tag{4.5.4}$$

对每个 $\sigma_N \in G$，有 $\lambda^{\sigma_N} = \rho_N(\lambda)$，$\rho_N(e(z)) = e(Nz)$（定理4.4.4). 于是对 $1 \leqslant i \leqslant q^d - 2$，有

$$\varphi_i(\lambda^{\sigma_N - 1}) = \frac{N}{e(Nz)} - \frac{1}{e(z)} \text{ 中 } z^{i-1} \text{ 的系数} \pmod P$$
$$\equiv (N^i - 1) B_i \Gamma_{i-1}/\Gamma_i \pmod P.$$

记 $\mathscr{P}$ 为 $F_{q^d} k = F_{q^d}(T)$ 中的素理想，$\mathscr{P} \mid P$. 而 θ 是 $\bmod \mathscr{P}$ 的 Teichmüller 特征，$\theta(\sigma_N) \equiv N \pmod P$，则对于

$$\chi_0 \neq \chi \in \hat{G}^+, \quad \varepsilon_\chi = \sum_{\sigma \in G} \bar{\chi}(\sigma)(\sigma - 1).$$

有
$$\varphi_i(\lambda^{\varepsilon_\chi}) \equiv \sum_{\sigma \in G} \bar{\chi}\theta^i(\sigma) B_i \Gamma_{i-1}/\Gamma_i \pmod P$$
$$\equiv \begin{cases} -B_i \Gamma_{i-1}/\Gamma_i \pmod P, & \text{若 } \chi = \theta^i; \\ 0, & \text{否则}. \end{cases}$$

但是当 $1 \leqslant i \leqslant q^d - 2$ 时，$P \nmid \Gamma_{i-1}\Gamma_i$. 这就表明了存在 i，$1 \leqslant i \leqslant$

$q^d-2,(q-1)\mid i$(即满足 $\chi=\theta$ 的 i),使得 $P\mid B_i$. 这就证明了定理 4.5.5. ▌

§ 4.6 循环函数域类数"奇偶性"

设 $k=\boldsymbol{F}_q(T)$,K/k 为 n 次循环扩张,$(n,q-1)=1$,并且有首1多项式 $M\in\boldsymbol{F}_q[T]$ 使得 $K\subseteq k(\Lambda_M)^+$. 我们说过:在函数域中 $q-1$ 对应于数域情况的偶数2. 本节中所谓类数 $h(K)$ 和 $h(O_K)$ 的奇偶性,是指它们是否能被 $q-1$ 的某个素因子 l 除尽. 我们要给出关于这个问题的一些初等判别法,很像是数域情形的讨论[13],[33].

以下固定 $q-1$ 的一个素因子 l,于是 $(n,l)=1$. 记 $C_y(K)$ 为 K 的分圆单位群,$C_K=\boldsymbol{F}_q^*C_y(K)$. 定理2.1.1表明了 $[U_K:C_K]=g(K)h(O_K)$,其中

$$g(K)=\prod_{\chi_0\neq\chi\in\hat{G}}\prod_{P\mid M}(1-\chi^*(P)).$$

现在假定

(Ⅰ) $(n,q-1)=1$, K/k 为 n 次循环扩张;

(Ⅱ) M 为域 K 的导子, $K\subseteq k(\Lambda_M)^+$;

(Ⅲ) 或者 n 为素数,或者 $M=P^t$.

在这些假设下可知 $g(K)=1$,于是

$$[U_K:C_K]=h(O_K). \tag{4.6.1}$$

我们引入 U_K 的一些子群(记为 $N=N_{K/k}$)如下:

$U_K^1=\{\varepsilon\in U_K:N(\varepsilon)=1\}$;

$U_K^{(l)}=\{\varepsilon\in U_K:N(\varepsilon)\in(\boldsymbol{F}_q^*)^l\}$;

$U_K^+=\{\varepsilon\in U_K:\varepsilon\in(K_{\mathscr{P}})^l$ (对 K 的每个无限素除子 $\mathscr{P}$)$\}$;

$(U_K)^l=\{\varepsilon^l:\varepsilon\in U_K\}$.

U_K — $U_K^{(l)}$ — U_K^+, U_K^1 — $(U_K)^l$

C_K — $C_K^{(l)}$ — C_K^+, C_K^1 — $(C_K)^l$

类似地有 C_K 的子群 C_K^1、$C_K^{(l)}$、C_K^+ 和 $(C_K)^l$.

由 $(l,n)=1$ 可知有如下的直积分解:

$U_K=U_K^1\times\boldsymbol{F}_q^*$, $U_K^{(l)}=U_K^1\times(\boldsymbol{F}_q^*)^l$,

$$C_K = C_K^1 \times \boldsymbol{F}_q^*, C_K^{(l)} = C_K^1 \times (\boldsymbol{F}_q^*)^l.$$

于是由(4.6.1)式可知

$$h(O_K) = [U_K^1 : C_K^1] = [U_K^{(l)} : C_K^{(l)}].$$

由于 $K \subseteq k(\Lambda_M)^+$，可知 k 的无限素除子∞在 K 中完全分裂为$\infty = \mathscr{P}_1 \cdots \mathscr{P}_n$. 现在给出 $l \mid h(O_K)$的一个判别法，其中 l 为 $q-1$的一个素因子.

定理4.6.1　设扩张 K/k 满足上述条件(Ⅰ)、(Ⅱ)和(Ⅲ). 则下列二条件等价：

(1) $l \mid h(O_K)$；

(2) 存在 l 次不分歧扩张 $K(\sqrt[l]{\alpha})/K$ $(\alpha \in K^*)$，使得 $\mathscr{P}_i (1 \leqslant i \leqslant n)$在 $K(\sqrt[l]{\alpha})$中均完全分裂.

证明　K 的 Hilbert 类域 $H(K)$是指 K 的最大不分歧阿贝尔扩张，使得 K 的每个无限素除子均完全分裂. Rosen[49]证明了：伽罗华群 Gal$(H(K)/K)$同构于 K 的理想类群. 再注意 $l \mid q-1$，从而 K 的 l 次阿贝尔扩张都是 Kummer 扩张. 由此即可证明定理 4.6.1. ▌

我们现在用分圆单位群来刻划 $l \mid h(O_K)$.

定理4.6.2　设扩张 K/k 满足条件(Ⅰ)、(Ⅱ)和(Ⅲ)，则下列三条件彼此等价：

(1) $l \nmid h(O_K)$；

(2) $C_K^+ \cap C_K^1 = (C_K^1)^l$；

(3) $C_K^+ = (C_K)^l$.

证明　(1)$\Leftrightarrow$(2)：若 $l \mid h(O_K) = [U_K^1 : C_K^1]$，则有 $\varepsilon \in U_K^1 - C_K^1$，使得 $\varepsilon^l \in C_K^1$. 于是 $\varepsilon^l \in (C_K^+ \cap C_K^1) - (C_K^1)^l$. 这表明了 $C_K^+ \cap C_K^1 \neq (C_K^1)^l$. 反之，设 $u \in (C_K^+ \cap C_K^1) - (C_K^1)^l$. 当 $u = \alpha^l, \alpha \in K^*$ 时，$\alpha \in U_K$. 我们可以取 $a \in \boldsymbol{F}_q^*, a^l = 1$，使得 $a\alpha \in U_K^1$. 于是 $a\alpha \notin C_K^1$ (否则，便会有 $u = (a\alpha)^l \in (C_K^1)^l$). 但是$(a\alpha)^l = u \in C_K^1$，所以 $l \mid [U_K^1 : C_K^1] = h(O_K)$. 如果 $u \notin (K^*)^l$，则 $K(\sqrt[l]{u})/K$ 是 l 次 Kummer 扩张. 由 $u \in U_K$ 可知 K 的每个有限素除子在 $K(\sqrt[l]{u})$中均不分歧. 由

$u\in C_K^+$可知K的每个无限素除子在$K(\sqrt[l]{u})$中均完全分裂. 于是$l|h(O_K)$(由定理4.6.1).

(2)$\Leftrightarrow$(3): 这是由于有直积分解$C_K^+=(C_K^+\cap C_K^1)\times(\boldsymbol{F}_q^*)^l$和$(C_K)^l=(C_K^1)^l\times(\boldsymbol{F}_q^*)^l$. ▌

以上定理告诉我们: $l\nmid h(O_K)$当且仅当$C_K^+=(C_K)^l$. 现在我们对于后者给出一个初等判别法:

首先固定K的一个无限素除子$\mathscr{P}$,则$K_{\mathscr{P}}=\boldsymbol{F}_q\left(\left(\frac{1}{T}\right)\right)$. 所以元素$\alpha\in K_{\mathscr{P}}^*$唯一表示为$\left(\frac{1}{T}\right)$-adic 展开:

$$\alpha=\sum_{\lambda\geqslant m}c_\lambda\left(\frac{1}{T}\right)^\lambda,\ c_\lambda\in\boldsymbol{F}_q,\ c_m\in\boldsymbol{F}_q^*,\ m=v_{\mathscr{P}}(\alpha).$$

我们记$\mathrm{sgn}(\alpha)=c_m$, 则 Hensel 引理给出:

$$\alpha\in(K_{\mathscr{P}}^*)^l\Leftrightarrow\mathrm{sgn}(\alpha)\in(\boldsymbol{F}_q^*)^l,\text{并且 }l|v_{\mathscr{P}}(\alpha).$$

所以对每个$\alpha\in K^*$,有

$$\begin{aligned}&\alpha\in(K_{\mathscr{P}'}^*)^l\quad(\text{对 }K\text{ 的每个无限素除子 }\mathscr{P}')\\&\Leftrightarrow\mathrm{sgn}(\tau(\alpha))\in(\boldsymbol{F}_q^*)^l\text{ 并且 }l|v_{\mathscr{P}}(\tau(\alpha))\\&\quad(\text{对每个 }\tau\in G=\mathrm{Gal}(K/k)).\end{aligned}$$

现在考虑商环

$$\Omega=\boldsymbol{F}_l[G]/(1+\sigma+\sigma^2+\cdots+\sigma^{n-1}),$$

其中σ为G的一个生成元. 由$(l,n)=1$可知Ω是半单代数,并且$\bar{C}_K^{(l)}=C_K^{(l)}/(C_K)^l$是$\Omega$-模. 我们把伽罗华群$\mathrm{Gal}(k(\Lambda_M)/k)$等同于$(R/(M))^*$,则$K$的固定子群等同于$(R/(M))^*$的子群$N$. 由$K\subseteq k(\Lambda_M)^+$可知$\boldsymbol{F}_q^*\subseteq N$. 我们取首1多项式集合$N'$,使得$N=N'\times\boldsymbol{F}_q^*$. 于是对每个$\alpha\in k(\Lambda_M)^+$,有

$$N_{k(\Lambda_M)^+/K}(\alpha)=\prod_{B\in N'}\sigma_B(\alpha).$$

由于$\mathrm{Gal}(K/k)=G\cong(R/(M))^*/N$是$n$阶循环群,可取$A\in R$,使得$\{1,A,A^2,\cdots,A^{n-1}\}$为$(R/(M))^*/N$的完全代表系,所以$\sigma=\sigma_A|_K$是$G$的一个生成元,而$C_K$是由$\boldsymbol{F}_q^*$和$\eta_i(0\leqslant i\leqslant n-2)$生成的,其中

$$\eta_i = N_{k(\Lambda_M)^+/K}(\sigma^i(\lambda^A/\lambda)) = N_{k(\Lambda_M)^+/K}(\lambda^{A^{i+1}}/\lambda^{A^i})$$
$$= \prod_{B\in N'}(\lambda^{A^{i+1}B}/\lambda^{A^iB}). \tag{4.6.2}$$

取 $\alpha\in F_q^*$，使 $\eta=\alpha\eta_0\in C_K^{(l)}$，易知

$$\overline{C}_K^{(l)} = \overline{\eta}^{\Omega}.$$

因为等式两端在 F_l 上的维数均是 $n-1$. 换句话说，$\overline{C}_K^{(l)}=C_K^{(l)}/(C_K)^l$ 是由 $\overline{\eta}$ 生成的忠实循环 Ω-模.

我们再固定一个非平凡同态：

$$\phi: F_q^*(\text{乘法群}) \to F_l(\text{加法群}),$$

并且考虑映射

$$S': \overline{C}_K^{(l)} \to F_l[X]/(X^n-1),$$
$$\overline{\varepsilon} \mapsto S'(\varepsilon,X) = \sum_{j=0}^{n-1} s(\varepsilon^{\sigma^j})X^{n-j-1} \pmod{X^n-1},$$

其中 $\varepsilon\in C_K^{(l)}$，$s(\varepsilon)=\phi(\mathrm{sgn}(\varepsilon))$. 由于 $\varepsilon\in C_K^{(l)}$，有

$$S'(\varepsilon,1) = \sum_{j=0}^{n-1} s(\varepsilon^{\sigma^j}) = s(N_{K/k}(\varepsilon)) = 0,$$

可知 $(X-1)\mid S'(\varepsilon,X)$. 于是诱导出同态：

$$S: \overline{C}_K^{(l)} \to F_l[X]/(1+X+\cdots+X^{n-1}),$$
$$\overline{\varepsilon} \mapsto S(\varepsilon,X) = S'(\varepsilon,X)/(X-1).$$

易知 $S(\overline{\varepsilon}^{\sigma})=XS(\overline{\varepsilon})$. 如果由 $f(X)^{\sigma}=Xf(X)$ 将 $F_l[X]/(1+X+\cdots+X^{n-1})$ 作成 Ω-模，则 S 是 Ω-模同态.

类似地，我们有另一个 Ω-模同态：

$$T: \overline{C}_K^{(l)} \to F_l[X]/(1+X+\cdots+X^{n-1}),$$
$$\overline{\varepsilon} \mapsto T(\varepsilon,X) = \sum_{j=0}^{n-1} t(\varepsilon^{\sigma^j})X^{n-j-1}/(X-1),$$

其中 $t(\varepsilon)\equiv v_{\mathfrak{P}}(\varepsilon) \pmod{l}$. 不难看出

$$\overline{C}_K^+(=C_K^+/(C_K)^l) = \mathrm{Ker}(S)\cap\mathrm{Ker}(T).$$

定理4.6.3　设 K/k 为 n 次循环扩张，并且满足条件(Ⅰ)、(Ⅱ)和(Ⅲ). 令

$$f_i(X)=S(\eta_i,X),\quad g_i(X)=T(\eta_i,X)\quad (0\leqslant i\leqslant n-2),$$

$$f(X)=(1+X+\cdots+X^{n-1},f_0(X),\cdots,f_{n-2}(X)),$$
$$g(X)=(1+X+\cdots+X^{n-1},g_0(X),\cdots,g_{n-2}(X)),$$

则 $l\nmid h(O_K)\Leftrightarrow(f(X),g(X))=1$.

证明 $I_m(S)$是由 $f_i(X)$ $(0\leqslant i\leqslant n-2)$生成的 $F_l[X]/(1+X+\cdots+X^{n-1})$的理想,所以是由 $f(X)$生成的主理想. 令

$$h(X)=(1+X+\cdots+X^{n-1})/f(X),$$

则

$$S(\bar{C}_K^{(l)h(\sigma)})=h(X)f(X)(F_l[X]/(1+X+\cdots+X^{n-1}))=(0).$$

这表明$(\bar{C}_K^{(l)})^{h(\sigma)}\subseteq\mathrm{Ker}(S)$. 但是

$$\dim_{F_l}(\bar{C}_K^{(l)})^{h(\sigma)}=\dim_{F_l}(\bar{\eta})^{h(\sigma)\Omega}=\dim_{F_l}h(\sigma)\Omega=\deg f(X),$$

$$\dim_{F_l}\mathrm{Ker}(S)=\dim_{F_l}(\bar{C}_K^{(l)})-\dim_{F_l}I_m(S)$$
$$=(n-1)-(n-1-\deg f)=\deg f.$$

所以 $\mathrm{Ker}(S)=\bar{\eta}^{h(\sigma)\Omega}$. 同样可知 $\mathrm{Ker}(T)=\bar{\eta}^{r(\sigma)\Omega}$,其中 $r(X)=(1+X+\cdots+X^{n-1})/g(X)$,于是

$$\bar{C}_K^+=\mathrm{Ker}(S)\cap\mathrm{Ker}(T)=\bar{\eta}^{l(\sigma)\Omega},$$

其中

$$l(X)=[h(X),r(X)]=\frac{1+X+\cdots+X^{n-1}}{(f(X),g(X))}.$$

于是 $\dim_{F_l}\bar{C}_K^+=\deg(f(X),g(X))$. 这就表明了

$$l\nmid h(O_K)\Longleftrightarrow C_K^+=(C_K)^l\quad(\text{定理 }4.6.2)$$
$$\Longleftrightarrow\bar{C}_K^+=(1)\Longleftrightarrow(f(X),g(X))=1.\qquad\blacksquare$$

定理4.6.3给出了 $l\mid h(O_K)$的一个判别方法,其中 $f(X)$和 $g(X)$是用分圆单位计算出来的多项式. 现在可以把这个计算化为更初等的方式. 对于 K 中无限素除子 $\mathscr{P}$,我们有 $k(\Lambda_M)$和 $k(\Lambda_M)^+$ 中无限素除子 $\mathfrak{P}$ 和 $\mathfrak{P}^+$,使得 $\mathfrak{P}^+\|\mathscr{P}$, $\mathfrak{P}^+=\mathfrak{P}^{q-1}$(见定理1.2.4). 令 $d=\deg M$,则有本原 M-torsion 元素 λ,使得对每个 $A'\in R$, $\deg A'\leqslant d-1$,均有

$$v_{\mathfrak{P}}(\lambda^{A'})=(q-1)(d-\deg A'-1)-1.$$

于是 $v_{\mathfrak{P}}(\lambda^{A'}/\lambda)=-(q-1)\deg A'$. $v_{\mathscr{P}}=v_{\mathfrak{P}^+}(\lambda^{A'}/\lambda)=-\deg A'$. 所以

$$t(\eta_i') = t\Big(\prod_{B\in N'}\lambda^{BA^{i+j+1}}/\lambda^{BA^{i+j}}\Big) \quad (见(6.2)式)$$
$$= \sum_{B\in N'} t\left(\frac{\lambda^{BA^{i+j+1}}/\lambda}{\lambda^{BA^{i+j}}/\lambda}\right)$$
$$= \sum_{B\in N'}(\deg[BA^{i+j}] - \deg[BA^{i+j+1}]), \quad (4.6.3)$$

其中对每个 $B\in R$,有$(B,M)=1$,这里$[B]$表示满足

$$[B]\equiv B \pmod M, \quad 0\leqslant \deg[B] < d$$

的多项式. 类似地,对于 $A'\in R$, $(A',M)=1$, $\deg A'<d$,有

$$\operatorname{sgn}(\lambda^{A'}/\lambda) = \operatorname{sgn}(A'\lambda/\lambda) = \operatorname{sgn}(A'),$$
$$s(\lambda^{A'}/\lambda) = s(A') = \phi(A' 的首项系数),$$
$$s(\eta_i') = \sum_{B\in N'}(s[BA^{i+j+1}] - s[BA^{i+j}]). \quad (4.6.4)$$

所以 $f_i(X)$和 $g_i(X)$可以按如下方式初等地计算出来:

定理4.6.4　设 K/k 是 n 次循环扩张,并且满足条件(Ⅰ)、(Ⅱ)和(Ⅲ);又设 $G=\mathrm{Gal}(K/k)=\langle\sigma_A\rangle$, $G(k(\Lambda_M)/K)\cong N$, $F_q^*\subseteq N\subseteq(R/(M))^*$, N'是 N/F_q^* 的完全代表系,则

$$(X-1)f_i(X) = \sum_{j=0}^{n-1}X^{n-j-1}\sum_{B\in N'}(s[BA^{i+j+1}] - s[BA^{i+j}]) \quad (0\leqslant i\leqslant n-2),$$
$$g_0(X) = -\sum_{j=0}^{n-1}X^{n-j-1}\sum_{B\in N'}\deg[BA^j],$$
$$g_i(X) = X^i g_0(X) \quad (1\leqslant i\leqslant n-2).$$

特别地,有 $g(X)=(1+X+\cdots+X^{n-1},g_0(X))$.

证明　第1个公式是由 $f_i(X)=S(\eta_i,X)$的定义和(4.6.4)式得出. 类似地,由(4.6.3)式可知:

$$(X-1)g_i(X) = \sum_{j=0}^{n-1}X^{n-j-1}\sum_{B\in N'}(\deg[BA^{i+j}] - \deg[BA^{i+j+1}]).$$

但是

$$\sum_{B\in N'}\deg[BA^i] = \sum_{B\in N'}\deg[BA^{i+n}],$$

所以

$$(X-1)g_i(X)=(X^i-X^{i+1})\sum_{j=0}^{n-1}X^{n-j-1}\sum_{B\in N'}\deg[BA^j].$$

由此即得 $g_0(X)$ 和 $g_i(X)$ $(1\leqslant i\leqslant n-2)$ 的表达式. ▌

以上证明了 $l\mid h(O_K)\Leftrightarrow \mathrm{Ker}(S)\cap\mathrm{Ker}(T)\neq(1)$. 对于除子类数 $h(K)$ 则有如下类似的结果:

定理4.6.5 设 K/k 是 n 次循环扩张,并且满足条件(Ⅰ)、(Ⅱ)和(Ⅲ),则

$$l\mid h(K)\Leftrightarrow \mathrm{Ker}(T)\neq(1).$$

证明 取 χ 是 $G=G(K/k)\cong(R/(M))^*/N$ 的特征群的生成元. 记 $\chi(A)=\zeta$(这是 n 次本原单位根). 由第1章的类数公式知

$$h(K)=\prod_{i=1}^{n-1}\sum_{\substack{C\in R_1\\ \deg C<d}}(-\chi^i(C)\deg C)$$

$$=\prod_{i=1}^{n-1}\Big(-\sum_{j=0}^{n-1}\sum_{B\in N'}\zeta^{i(n-j)}\deg[BA^j]\Big).$$

记 $\mathscr{P}$ 为 l 到 $\boldsymbol{Q}(\zeta)$ 中一个扩充素理想,则

$l\mid h(K)\Leftrightarrow$ 存在 i $(1\leqslant i\leqslant n-1)$,使得

$$\sum_{j=0}^{n-1}\sum_{B\in N'}\zeta^{i(n-j)}\deg[BA^j]\equiv 0 \pmod{\mathscr{P}}$$

$\Leftrightarrow$ 对于域 $\boldsymbol{Z}[\zeta]/\mathscr{P}$ 中的某个 n 次本原单位根 w,有 $g_0(W)=0$

$\Leftrightarrow g(X)=(1+X+\cdots+X^{n-1},g_0(X))\neq 1$

$\Leftrightarrow \mathrm{Ker}(T)\neq(1)$. ▌

特别地,对于 $M=P$ 的情形,$f(X)$ 和 $g(X)$ 可按如下方式计算:

定理4.6.6 设 K/k 为 n 次循环扩张,满足条件(Ⅰ)和(Ⅱ),并且 $M=P$ 是 $R=\boldsymbol{F}_q[T]$ 中 d 次首1不可约多项式. 取 $\alpha\in R$ 是循环群 $(R/(P))^*\cong\boldsymbol{F}_{q^d}^*$ 的一个生成元. 令 $m=[k(\Lambda_P)^+:K]$ $\left(从而\ mn=[k(\Lambda_P)^+:k]=\dfrac{q^d-1}{q-1}\right)$,

$$f'(X)=\sum_{j=0}^{n-1}X^{n-j-1}\sum_{r=0}^{m-1}s[\alpha^{rn+j}],$$

$$g_0(X) = -\sum_{j=0}^{n-1} X^{n-j-1} \sum_{r=0}^{m-1} \deg[\alpha^{nr+j}],$$

则 $f(X) = (1 + X + X^2 + \cdots + X^{n-1}, (X-1)f'(X) + 1)$,

$g(X) = (1 + X + X^2 + \cdots + X^{n-1}, g_0(X))$.

证明　关于 $g_0(X)$ 和 $g(X)$ 的公式由定理4.6.4给出. 另一方面,我们有

$$(X-1)f_i(X) = \sum_{j=0}^{n-1} X^{n-j-1} \sum_{r=0}^{m-1} (s[\alpha^{nr+j+i+1}] - s[\alpha^{nr+j+i}]).$$

当 $nm \leqslant t \leqslant 2nm-1$ 时,有

$$\begin{aligned} s[\alpha^t] &= s[a\alpha^{t-mn}] = s(a) + s[\alpha^{t-mn}] \\ &= \phi(a) + s[\alpha^{t-mn}] = s[\alpha^{t-mn}] + 1, \end{aligned}$$

其中 $a = \alpha^{\frac{q^d-1}{q-1}}$ 是 F_q^* 的生成元. 于是

$$\begin{aligned} (X-1)f_i(X) &= (X^{i+1} - X^i)\left(\sum_{j=0}^{n-1} X^{n-j-1} \sum_{r=0}^{m-1} s[\alpha^{nr+j}]\right) \\ &\quad + \sum_{j=n-i-1}^{n-1} X^{n-j-1} - \sum_{j=n-i}^{n-1} X^{n-j-1} \\ &= X^i((X-1)f'(X) + 1) \quad (0 \leqslant i \leqslant n-2), \end{aligned}$$

于是

$$\begin{aligned} f(X) &= (1 + X + \cdots + X^{n-1}, f_0(X), f_1(X), \cdots, f_{n-2}(X)) \\ &= (1 + X + \cdots + X^{n-1}, (X-1)f'(X) + 1). \end{aligned}$$ ∎

定理4.6.7　设 K/k 为 n 次循环扩张,并且满足条件(Ⅰ)、(Ⅱ)和(Ⅲ)′ $n=p$ 为奇素数,并且 l 为 F_q^* 的生成元.

又令 $t_j = -\sum_{B \in N'} \deg[BA^j]$ $(0 \leqslant j \leqslant p-1)$,则

$$l \mid h(K) \Longleftrightarrow t_0 \equiv t_1 \equiv \cdots \equiv t_{p-1} \pmod{l}.$$

又若 $M=P$, $d=\deg P$, $\frac{q^d-1}{q-1}=pm$, α 为 $(R/(P))^* \cong F_{q^d}^*$ 的生成元. 记

$$s_j = \sum_{r=0}^{m-1} s[\alpha^{pr+j}],\quad t_j = -\sum_{r=0}^{m-1} \deg[\alpha^{pr+j}] \quad (0 \leqslant j \leqslant p-1),$$

则

$$l \mid h(K) \Longleftrightarrow t_0 \equiv t_1 \equiv \cdots \equiv t_{p-1} \pmod{l},$$

$$l \mid h(O_K) \Longleftrightarrow l \mid h(K) \quad \text{并且} \quad s_j \equiv s_0 + \frac{j}{p} \pmod{l}$$
$$(1 \leqslant j \leqslant p-1).$$

证明 我们有 $g_0(X)=\sum_{j=0}^{p-1} t_j X^{p-j-1}$，而条件(Ⅱ')表明了 $1+X+\cdots+X^{p-1}$ 在 $\boldsymbol{F}_l[X]$ 中是不可约的. 于是有

$$\begin{aligned} l \mid h(K) &\Longleftrightarrow (1+X+\cdots+X^{p-1}, g_0(X)) \neq 1 \quad (\text{在 } \boldsymbol{F}_l[X] \text{ 中}) \\ &\Longleftrightarrow 1+X+\cdots+X^{p-1} \mid g_0(X) \quad (\text{在 } \boldsymbol{F}_l[X] \text{ 中}) \\ &\Longleftrightarrow t_0 \equiv t_1 \equiv \cdots \equiv t_{p-1}' \pmod{l}. \end{aligned}$$

另一方面，

$$\begin{aligned} (X-1)f'(X)+1 = & (X-1)+(s_{p-1}+s_{p-2}X+\cdots \\ & + s_0 X^{p-1})+1 \\ \equiv & (1+s_0-s_{p-1})+(s_{p-1}-s_{p-2})X+\cdots \\ & + (s_1-s_0)X^{p-1} \pmod{X^p-1}. \end{aligned}$$

所以

$$\begin{aligned} & 1+X+\cdots+X^{p-1} \mid (X-1)f'(X)+1 \\ & \Longleftrightarrow 1+s_0-s_{p-1} \equiv s_{p-1}-s_{p-2} \equiv \cdots \equiv s_1-s_0 \pmod{l} \\ & \Longleftrightarrow s_j \equiv s_0 + \frac{j}{p} \pmod{l} \quad (1 \leqslant j \leqslant p-1). \end{aligned}$$ ∎

第 5 章

分 析 学

§5.1 连 续 函 数

设 C_p 为 p-adic 数域 $\boldsymbol{Q}_p$ 的代数闭包，古典的 Mahler 定理是说：每个连续函数 $f:\boldsymbol{Z}_p\to C_p$ 均可唯一地表示成

$$f(x)=\sum_{n\geqslant 0}a_n\binom{x}{n},$$

其中 $a_n\in C_p, a_n\to 0$ （对于 p-adic 拓扑）.

本节的目的是给出这一结果在函数域情形的模拟.

设 $q=p^m$，$R=\boldsymbol{F}_q([T])$，$k=\boldsymbol{F}_q(T)$，$k_\infty=\boldsymbol{F}_q\left(\left(\frac{1}{T}\right)\right)$，$k$ 上对 $\infty=\left(\frac{1}{T}\right)$ 的标准指数赋值 v_∞ 唯一地扩充到 k_∞ 的代数闭包 k_∞^{ac} 之上. 我们在第 3 章曾引入了：

$[i]=T^{q^i}-T \quad (i\geqslant 1)$；

$D_0=1,\ D_i=D_{i-1}^q\cdot[i]=[i][i-1]^q\cdots[1]^{q^{i-1}} \quad (i\geqslant 1)$；

$L_0=1,\ L_i=[i][i-1]\cdots[1] \quad (i\geqslant 1)$.

则 $D_i=\prod\limits_{\substack{A\in R_1\\ \deg A=i}}A$，其中 R_1 表示 R 中首 1 多项式全体.

又令
$$e_i(x)=\prod_{\substack{A\in R\\ \deg A<i}}(x-A)\quad (i\geqslant 0),$$

这是系数属于 R 的关于变量 x 的 q-线性多项式. 事实上，我们有

$$e_i(x) = \sum_{j=0}^{i}(-1)^{i-j}\begin{bmatrix} i \\ j \end{bmatrix} x^{q^j}, \tag{5.1.1}$$

其中

$$\begin{bmatrix} i \\ j \end{bmatrix} = \begin{cases} D_i/D_jL_{i-j}^{q^j}, & \text{若 } j \leqslant i; \\ 0, & \text{否则}. \end{cases}$$

现在引入"差分"算子. 设 K 是 k 的某个扩域.

定义 对于 q-线性多项式 $f(x)=\sum\limits_{n\geqslant 0} c_n x^{q^n} \in K[x]$, 令

$$\Delta f(x) = \Delta^{(1)}f(x) = f(Tx) - Tf(x),$$

$$\Delta^{(i)}f(x) = \Delta^{(i-1)}f(Tx) - T^{q^{i-1}}\Delta^{(i-1)}f(x) \quad (i \geqslant 2).$$

引理 5.1.1 (i) $\Delta^{(j)}(x^{q^l}) = \prod\limits_{k=0}^{j-1}(T^{q^l}-T^{q^k}) \cdot x^{q^l}$. 特别是, 若 $\deg f(x) \leqslant q^{j-1}$, 则 $\Delta^{(j)}f(x)=0$.

(ii) $\Delta^{(j)}e_i(x) = \dfrac{D_i}{D_{i-j}^{q^j}} e_{i-j}^{q^j}(x)$.

证明 (i) 可由定义直接验证之.

(ii) 当 $j>i$ 时, 等式两端均为 0(因为 $\deg e_i(x)=q^i$). 以下设 $j\leqslant i$. 由于(5.1.1)式和本引理的(i)可知

$$\Delta^{(j)}e_i(x) = \sum_{l=0}^{i}(-1)^{i-l}\frac{D_i}{D_lL_{i-l}^{q^l}}\left(\prod_{k=0}^{j-1}\left(T^{q^l}-T^{q^k}\right)\right)x^{q^l},$$

另一方面,

$$\frac{D_i}{D_{i-j}^{q^j}}e_{i-j}^{q^j}(x) = \frac{D_i}{D_{i-j}^{q^j}}\sum_{l=0}^{i-j}(-1)^{i-j-l}\frac{D_{i-j}^{q^j}}{D_l^{q^j}L_{i-j-l}^{q^{l+j}}}x^{q^{l+j}}.$$

所以只需证明: 对于 $0\leqslant l\leqslant i-j$, 有

$$\frac{D_i}{D_{l+j}L_{i-l-j}^{q^{l+j}}}\prod_{k=0}^{j-1}\left(T^{q^{l+j}}-T^{q^k}\right) = \frac{D_i}{D_{i-j}^{q^j}}\cdot\frac{D_{i-j}^{q^j}}{D_l^{q^j}L_{i-j-l}^{q^{l+j}}},$$

即 $D_{l+j}=D_l^{q^j}\prod\limits_{k=0}^{j-1}\left(T^{q^{l+j}}-T^{q^k}\right)$. 这可由 D_i 的定义直接推出. ▌

由于对每个 $j\geqslant 0$, $e_j(x)$ 是 q^j 次首 1 的 q-线性多项式, 所以每个 q-线性多项式 $f(x)\in K[x]$($\deg f(x)=q^i$)均可唯一的表示成

$$f(x)=\sum_{j=0}^{i}b_je_j(x),b_j\in K.$$

引理 5.1.2　对于 $u\in K$，则 $f(ux)=\sum_{j=0}^{i}b_j(u)e_j(x)$，其中 $b_j(u)=\frac{\Delta^{(j)}f(u)}{D_j}$.

证明　由 $\Delta^{(j)}f(ux)=\sum_{t=0}^{i}b_t(u)\Delta^{(j)}e_t(x)$

$$=\sum_{t=0}^{i}b_t(u)\frac{D_t}{D_{t-j}^{q^j}}e_{t-j}^{q^j}(x),$$

再由 $e_t(1)=0$（当 $t\neq0$ 时），$e_0(1)=1$，可知 $\Delta^{(j)}f(u)=b_j(u)D_j$. 证毕.　▌

对每个非负整数 $j\geqslant0$，记 $j=\sum_{i=0}^{s}\alpha_iq^i$ 为 q-adic 展开. 在上一章曾介绍过 Gamma 函数 $\Gamma_j=\prod_{i=0}^{s}D_i^{\alpha_i}$ 作为阶乘函数 $n!$ 的模拟.

现在给出以下定义：

定义　$G_j(x)=\prod_{i=0}^{s}e_i(x)^{\alpha_i}$ 称作 Carlitz 函数.

注意 $G_j(x)$ 是 j 次首 1 多项式，系数属于 k. 所以对于每个 d 次多项式 $f(x)\in K[x]$（其中 K 为 k 的某个扩域），则可唯一表达成

$$f(x)=\sum_{j=0}^{d}b_jG_j(x),b_j\in K.$$

下面确定系数 b_j.

定理 5.1.3　设 $j=\sum_{i=0}^{s}\alpha_iq^i$ 为 q-adic 展开. 记

$$g_{\alpha_iq^i}(x)=\begin{cases}e_i^{\alpha_i}(x)，若 0\leqslant\alpha_i<q-1；\\ e_i^{\alpha_i}(x)-D_i^{q-1}，若 \alpha_i=q-1.\end{cases}$$

再令 $g_j(x)=\prod_{i=0}^{s}g_{\alpha_iq^i}(x)$，则当 $q^m>j$ 时，

$$b_j=(-1)^m\frac{L_m}{D_m}\sum_{\substack{A\in R\\ \deg A<m}}g_{q^m-1-j}(A)f(A).$$

在证明定理 5.1.3 之前，先作如下准备：

引理 5.1.4 （1）加法公式：

$$G_j(x+u)=\sum_{e+f=j}G_e(x)G_f(u)\binom{j}{e};$$

$$\frac{G_j(x+u)}{\Gamma_j}=\sum_{e+f=j}\frac{G_e(x)}{\Gamma_e}\cdot\frac{G_f(u)}{\Gamma_f}\binom{j}{e};$$

$$g_j(x+u)=\sum_{e+f=j}\binom{j}{e}G_e(x)g_f(u).$$

（2）当 $A\in R$ 时，$G_j(A)/\Gamma_j\in R$，$g_j(A)/\Gamma_j\in R$.

（3）若 $f(x)\in K[x]$，$\deg f=d<q^m$，则

$$(-1)^m\frac{D_m}{L_m}f(x)=\sum_{\substack{A\in R\\ \deg A<m}}f(A)\frac{e_m(x)}{x-A}.$$

证明 （1）$G_j(x+u)=\prod_{i=0}^{s}(e_i(x)+e_i(u))^{\alpha_i}$

$$=\prod_{i=0}^{s}\sum_{\beta_i=0}^{\alpha_i}\binom{\alpha_i}{\beta_i}e_i(x)^{\beta_i}\cdot e_i(u)^{\alpha_i-\beta_i}$$

$$=\sum_{\beta_1=0}^{\alpha_1}\cdots\sum_{\beta_s=0}^{\alpha_s}\binom{\alpha_1}{\beta_1}\cdots\binom{\alpha_s}{\beta_s}G_\beta(x)\cdot G_{j-\beta}(u)$$

$$=\sum_{\beta=0}^{j}\binom{j}{\beta}G_\beta(x)\cdot G_{j-\beta}(u).$$

类似地可证明第二个等式. 最后

$$g_j(x+u)=\sum_{i=0}^{s}g_{\alpha_iq^i}(x+u)$$

当 $\alpha_i<q-1$ 时，

$$g_{\alpha_iq^i}(x+u)=(e_i(x)+e_i(u))^{\alpha_i}$$

$$=\sum_{\beta_i=0}^{\alpha_i}\binom{\alpha_i}{\beta_i}G_{q^i}(x)^{\beta_i}g_{q^i}(u)^{\alpha_i-\beta_i}.$$

而当 $\alpha_i=q-1$ 时，

$$g_{(q-1)q^i}(x+u)=(e_i(x)+e_i(u))^{q-1}-D_i^{q-1}$$

$$= \sum_{\beta_i=0}^{\alpha_i} \binom{\alpha_i}{\beta_i} G_{q^i}(x)^{\beta_i} g_{q^i}(u)^{\alpha_i-\beta_i}.$$

然后就可证明第三个等式.

(2) 我们只需证明 $e_i(A)/D_i \in R$，当 $\deg A < i$ 时，$e_i(A)=0$. 下设 $\deg A \geqslant i$. 这时

$$e_i(A) = \prod_{\substack{B\in R \\ \deg B < i}} (A-B), \quad D_i = \prod_{\substack{A\in R_1 \\ \deg A = i}} A.$$

对每个 s 次首 1 不可约多项式 P，有

$$v_P(D_i) = \sum_{\substack{k\geqslant 0 \\ i-ks\geqslant 0}} q^{i-ks} \leqslant v_P(e_i(A)).$$

因此 $e_i(A)/D_i \in R$.

(3) 将等式右端记为 $h(x)$，则 $\deg h(x) \leqslant q^m - 1$. R 中共有 q^m 个次数小于 m 的多项式 A. 对每个这样的 A，有

$$h(A) = f(A)\frac{e_m(x)}{x-A}\bigg|_{x=A} = f(A)\frac{e_m(x-A)}{x-A}\bigg|_{x=A}$$

$$= f(A)\frac{e_m(x)}{x}\bigg|_{x=0} = (-1)^m \frac{D_m}{L_m} f(A) \quad (\text{由}(5.1.1)\text{式}).$$

即(3)中公式两端在 x 的 q^m 个值上有相同的函数值. 所以它们相等. ∎

定理 5.1.3 的证明　取 m 使 $q^m > d$. 则

$$(-1)^m \frac{D_m}{L_m} f(x) = \sum_{\substack{A\in R \\ \deg A < m}} f(A)\frac{e_m(x-A)}{x-A}$$

(由引理 5.1.4 的(3)).

但是由于

$$g_{q^m-1}(x) = \prod_{i=0}^{m-1} (e_i^{q-1}(x) - D_i^{q-1}),$$

$$e_i^{q-1}(x) - D_i^{q-1} = \prod_{\substack{A\in R \\ \deg A = i}} (x-A),$$

(第二个等式是由于两端均为 x 的 $(q-1)q^i$ 次首 1 多项式，并且当 $x = A\in R(\deg A = i)$时两端取值均为 0.)因此

$$g_{q^m-1}(x)=\prod_{\substack{A\in R\\ 0\leqslant \deg A<m}}(x-A)=\frac{e_m(x)}{x}.$$

所以

$$(-1)^m\frac{D_m}{L_m}f(x)=\sum_{\substack{A\in R\\ \deg A<m}}f(A)g_{q^m-1}(x-A)$$

$$=\sum_{\substack{A\in R\\ \deg A<m}}f(A)\sum_{i+j=q^m-1}G_j(x)g_i(A)\quad(\text{加法公式}).$$

由分解的唯一性可知对每个 $m,q^m>d$ 均有

$$b_j=(-1)^m\frac{L_m}{D_m}\sum_{\deg A<m}f(A)g_{q^m-1-j}(A).$$

以下还需证明：当 $q^{m-1}>j$ 时，必然有

$$(-1)^m\frac{L_m}{D_m}\sum_{\deg A<m}f(A)g_{q^m-1-j}(A)$$

$$=(-1)^{m-1}\frac{L_{m-1}}{D_{m-1}}\sum_{\deg A<m-1}f(A)g_{q^{m-1}-1-j}(A).\tag{5.1.2}$$

由于

$$\frac{L_m}{D_m}=\frac{L_{m-1}[m]}{D_{m-1}^q[m]},\quad q^m-1-j=q^{m-1}-1-j+(q-1)q^{m-1},$$

所以(5.1.2)式等价于

$$\sum_{\deg A<m}f(A)g_{q^{m-1}-1-j}(A)\left(e_{m-1}^{q-1}(A)-D_{m-1}^{q-1}\right)$$

$$=-D_{m-1}^{q-1}\sum_{\deg A<m-1}f(A)g_{q^{m-1}-1-j}(A).$$

这又等价于

$$\sum_{\deg A=m}f(A)g_{q^{m-1}-1-j}\left(e_{m-1}^{q-1}(A)-D_{m-1}^{q-1}\right)=0.$$

但是当 $\deg A=m$ 时，$e_{m-1}(A)=D_{m-1}$. 所以上式成立. 所以(5.1.2)式也成立. 由(5.1.2)式可知定理 5.1.3 中 b_j 的公式对于满足 $q^m>j$的每个 m 均成立. 这就完成了定理 5.1.3 的证明. ▌

现在可以叙述 Mahler 定理的模拟了. 引理 5.1.4 的(2)表明

了：函数 $G_j(x)/\Gamma_j$ 是从 R 到 R 的映射. 现在设 P 是 $R=F_q[T]$ 中一个固定的首 1 不可约多项式，$R_P=\{\alpha\in k_P: v_P(\alpha)\geqslant 0\}$ 是 R 在 P 处的局部环. 令 $d=\deg P$，当 $t\geqslant j$ 时，

$$v_P(D_j)=q^{j-d}+q^{j-2d}+\cdots,$$
$$v_P(e_j(AP^t))\geqslant t+q^{j-d}+q^{j-2d}+\cdots.$$

于是

$$v_P(e_j(AP^t)/D_j)\geqslant t.$$

这就表明了：当 x、$y\in R$，并且 $v_P(x-y)=t\geqslant j$ 时，

$$v_P\left(\frac{G_j(x)}{\Gamma_j}-\frac{G_j(y)}{\Gamma_j}\right)\geqslant t.$$

于是我们可把 $G_j(x)/\Gamma_j$ 扩充成从 R_P 到 R_P 的连续函数：

$$G_j(x)/\Gamma_j:\ R_P\to R_P.$$

定理 5.1.5　(Carlitz)　设 C_P 是 k_P 的代数闭包，K 为 k_P 的扩域，$K\subseteq C_P$，K 赋以由 P-adic 赋值诱导的拓扑. 则

(1) 每个连续函数 $f: R_P\to K$ 可唯一表示成

$$f(x)=\sum_{j\geqslant 0}a_j\frac{G_j(x)}{\Gamma_j},\tag{5.1.3}$$

其中 $a_j\in K$，$a_j\to 0$.

(2) 反之，对于 $a_j\in K$，$a_j\to 0$，则由(5.1.3)给出的 f 必为R_P 到 K 的连续函数.

证明　由于当 $x\in R_P$ 时，$G_j(x)/\Gamma_j\in R_P$. 所以(2)是显然的. 现在证明(1). 对每个 $m\geqslant 0$，令 $f_m(x)$ 是唯一的次数$\leqslant q^m-1$ 的多项式，使得对每个 $A\in R$，$\deg A<m$，均有 $f_m(A)=f(A)$. 由定理 5.1.3 知道

$$f_m(x)=\sum_{j=0}^{q^m-1}b_j^{(m)}G_j(x),$$

其中

$$b_j^{(m)}=(-1)^m\frac{L_m}{D_m}\sum_{\substack{A\in R\\ \deg A<m}}g_{q^m-1-j}(A)f(A).$$

因为 $b_j^{(m)}=b_j^{(m+1)}=\cdots$，所以可把它们记成 b_j. 接着只需再证 $a_j=$

$b_j\Gamma_j \to 0$ 即可.

对每个 j,有 m 使得 $q^m > j \geqslant q^{m-1}$,于是

$$a_j = (-1)^m \frac{L_m}{D_m}\Gamma_j\Gamma_{q^m-1-j}\sum_{\deg A<m}\frac{g_{q^m-1-j}(A)}{\Gamma_{q^m-1-j}}f(A).$$

当 $A\in R\subseteq R_P$ 时,$f(A)\in R_P$. 进而又知道 $g_{q^m-1-j}(A)/\Gamma_{q^m-1-j}\in R$ (根据引理 5.1.4 的(2)),并且 $\Gamma_j\Gamma_{q^m-1-j}=(D_0D_1\cdots D_{m-1})^{q-1}=\frac{D_m}{L_m}$,所以

$$a_j = (-1)^m \sum_{\deg A<m} h(A),$$

其中 $h(x)=g_{q^m-1-j}(x)f(x)/\Gamma_{q^m-1-j}$是 x 的有界连续函数. 于是对每个 $N>0$,均有 s 使 $v_P(\alpha-\beta)\geqslant s$ 时,必然有 $v_P(h(\alpha)-h(\beta))\geqslant N$. 现在取 j 充分大,使 $m>ds$,则

$$\begin{aligned} a_j &= (-1)^m \sum_{\substack{\deg B<m-sd\\ \deg C<sd}} h(BP^s+C) \\ &= (-1)^m \sum_{B,C}(h(BP^s+C)-h(C)), \end{aligned}$$

所以 $v_P(a_j)\geqslant N$. 这就证明了 $a_j\to 0$. 从而

$$f(x)=\lim f_m(x)=\sum_{j\geqslant 0}a_jG_j(x)/\Gamma_j. \qquad \blacksquare$$

§5.2 P-adic Gamma 函数

古典的 Gamma 函数是由下面积分定义的复值函数

$$\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}dt.$$

这个积分在 $\mathrm{Re}(z)>0$ 中收敛,由于对每个正整数 n 有 $\Gamma(n)=(n-1)!$,所以 $\Gamma(z)$是阶乘函数的解析扩充. 这个函数有如下基本性质:

(1) 递推公式 $\Gamma(z+1)=z\Gamma(z)$

由这个公式可以把 $\Gamma(z)$扩充成整个复平面上的亚纯函数,它在 C 中没有零点,极点为 $z=0,-1,-2,\cdots$,并且均是单极点,在 $z=-n$处的留数为 $\operatorname{res}\limits_{z=-n}\Gamma(z)=(-1)^n\frac{1}{n!}$, $\Gamma(z)^{-1}$为整个复平面上的

全纯函数.

(2) Gauss 乘积公式　对每个正整数 n，有

$$\Gamma(z)\Gamma\left(z+\frac{1}{n}\right)\cdots\Gamma\left(z+\frac{n-1}{n}\right)=(2\pi)^{\frac{n-1}{2}}n^{\frac{1}{2}-nz}\Gamma(nz).$$

(3) 函数方程 $\Gamma(z)\Gamma(1-z)=\pi/\sin\pi z$

特别取 $z=\frac{1}{2}$，得到 $\Gamma\left(\frac{1}{2}\right)=\sqrt{\pi}$. 再由递推公式可计算出 $\Gamma\left(n+\frac{1}{2}\right)$ $(n=1,2,\cdots)$的值，它们均是 $\sqrt{\pi}$ 乘以非零有理数.

函数 $\Gamma(z)$作为一类特殊函数最早应用到微分方程和物理学中. 它的数论意义有以下几方面：

(A) 它和黎曼 zeta 函数 $\zeta(s)=\sum_{n\geqslant 1}n^{-s}$的联系为

$$\Gamma(s)\zeta(s)=\int_0^{\infty}t^{s-1}(e^t-1)^{-1}dt\quad(\mathrm{Re}s>1).$$

由此出发可得到 $\zeta(s)$的函数方程和解析开拓. 更一般地，对于任意代数数域 K，zeta 函数 $\zeta_K(s)$的函数方程中的 Γ-因子反映了 K 中无限素除子的性状.

(B) $\Gamma(s)$在有理点 $s\in Q$ 处的取值有深刻的数论含义. Deligne 猜想 $\Gamma(s)$在某些有理点处取值的适当组合是代数数，并且生成某些分圆域的 Abel 扩张. 这个猜想后来由 Koblitz-Ogus 所证明.

Gamma 函数 $\Gamma(z)$的 P-adic 模拟最早是由 Morita 引进的. 为了保证 $n!$ 在 Q_p 中有良好的性状，需要去掉阶乘中被 P 除尽的那些因子，即令

$$\Gamma_p(n)=(-1)^n\prod_{\substack{j=1\\ p\nmid j}}^{n-1}j\quad(n=1,2,3,\cdots).$$

于是 $\Gamma_p(1)=-1$，$\Gamma_p(2)=1$. 不难证明：若正整数 n 和 m 的P-adic距离很小，则 $\Gamma_p(n)$和 $\Gamma_p(m)$的P-adic距离也很小. 由于正整数集合在 Z_p 中是稠密的，这就定义出P-adic连续函数

$$\Gamma_p:Z_p\to Z_p^*=\{\alpha\in Z_p:v_p(\alpha)=0\}=Z_p-pZ_p.$$

函数 $\Gamma_p(z)$ $(z\in Z_p)$有与 $\Gamma(z)$类似的一些性质（详见 Lang S 的书

——文献[45]).

(A_p) 递推公式

$$\Gamma_p(z+1)=\begin{cases}-z\Gamma_p(z), 若 z\in Z_p^*;\\ -\Gamma_p(z), 若 z\in pZ_p.\end{cases}$$

(B_p) 乘积公式　若 $P\nmid n\geqslant 2$,则

$$\prod_{i=0}^{n-1}\Gamma_p\left(\frac{z+i}{n}\right)=\Gamma_p(z)\alpha(n)g_n(z)^{-1},$$

其中 $\alpha(n)^4=1$，$g_n(z)$为 n 的某个 P-adic 方幂.

(C_p) 函数方程　$\Gamma_p(z)\Gamma_p(1-z)=\pm 1$.

当 $p>2$ 时,$\frac{1}{2}\in Z_p$. 由函数方程可知 $\Gamma_p\left(\frac{1}{2}\right)^4=1$. 再由递推公式可知对每个整数 n，$\Gamma_p\left(n+\frac{1}{2}\right)^4$ 均是有理数.

为了与下面要讲的函数域情形对比,在此只介绍函数 $\Gamma_p(z)$ 的一个数论应用,即用 $\Gamma_p(z)$在有理点处的一些特殊值来表示 Gauss 和.

设 $q=p^f$，p 为素数. 以 T 表示扩张 F_q/F_p 的迹函数:

$$T:F_q\rightarrow F_p, T(\alpha)=\alpha+\alpha^p+\alpha^{p^2}+\cdots+\alpha^{p^{f-1}}.$$

F_q 的加法特征是加法群 F_q 到复数乘法群 C^* 的同态. 例如对每个 $\alpha\in F_q$　(对每个正整数 n,令 $\zeta_n=e^{\frac{2\pi i}{n}}$),

$$\psi_\alpha:F_q\rightarrow F_p,\ \psi_\alpha(\beta)=\zeta_p^{T(\alpha\beta)}$$

是 F_q 的加法特征. 熟知$\{\psi_\alpha:\alpha\in F_q\}$就是 F_q 的全部加法特征. F_q 的乘法特征是指乘法群 F_q^* 到 C^* 的同态. 由于 F_q^* 是 $q-1$ 阶循环群,所以每个乘法特征的取值均为 $q-1$ 次单位根,即属于$\langle\zeta_{q-1}\rangle$. 在 $Q(\zeta_{q-1})$的整数环 $Z[\zeta_{q-1}]$中取定一个素理想 $\mathscr{P}$,使得$\mathscr{P}|p$,则 $Z[\zeta_{q-1}]/\mathscr{P}=F_q$. 熟知 F_q 有唯一的乘法特征 $\omega:F_q^*\rightarrow\langle\zeta_{q-1}\rangle$,使得对每个 $\alpha\in F_q^*$,有 $\omega(\alpha)\equiv\alpha\pmod{\mathscr{P}}$. ω 称作 Teichmüller 特征,而 F_q 的所有乘法特征为 $\chi_0=\omega^0,\omega^1,\cdots,\omega^{q-2}$.

设 ψ_a 和 χ 分别为 F_q 的加法特征和乘法特征,我们称

$$g(\chi,\psi_a)=-\sum_{\alpha\in F_q^*}\chi(\alpha)\psi_a(\alpha)=-\sum_{\alpha\in F_q^*}\chi(\alpha)\zeta_p^{T(a\alpha)}\in Z[\zeta_{q-1},\zeta_p]为$$

Gauss 和. 易知

$$g(\chi,\psi_0)=\begin{cases}-(q-1), & 若\ \chi=\chi_0;\\ 0, & 若\ \chi\neq\chi_0.\end{cases}$$

而当 $a\in F_q^*$ 时,$g(\chi,\psi_a)=\overline{\chi}(a)\cdot g(\chi_1,\psi_1)$. 所以只需研究 $g(\chi,\psi_1)$ 即可. 我们把它记为 $g(\chi)$. 所以本质上只需研究 $g(\omega^a)$ $(1\leqslant a\leqslant q-2)$ (注意 $g(\omega^0)=1$).

易证

$$g(\omega^a)\cdot\overline{g(\omega^a)}=q=p^f.$$

但是当 ω^a 不是二阶特征时,$g(\omega^a)$的确切值是很难求得的. 现在设 m 为 $q-1$的一个因子,$q-1=md$,则 ω^{-d}是F_q的 m 阶乘法特征. 可以证明 $g(\omega^{-d})^m\in Q(\zeta_m)$. 我们现在求主理想$(g(\omega^{-d})^m)$在环$Z[\zeta_m]$中的素理想分解式. 记$\mathscr{P}$为$Z[\zeta_{q-1}]$中素理想$\mathscr{P}$在$Z[\zeta_m]$中的限制. 则$\mathscr{P}$的共轭理想有形式$\mathscr{P}^{\sigma_a}$,其中$(a,m)=1$,而$\sigma_a$是$Q(\zeta_m)$的自同构,使$\sigma_a(\zeta_m)=\zeta_m^a$. 由于 $g(\omega^a)\cdot\overline{g(\omega^a)}=p^f$,可知$(g(\omega^{-d})^m)$的每个素理想因子都是 $\mathscr{P}$ 的共轭理想.

Stickelberger 引理 $(g(\omega^{-d})^m)=\mathscr{P}^\theta$, $\theta=\sum\limits_{\substack{a=1\\(a,m)=1}}^{m}a\sigma_a^{-1}$.

换句话说,$\mathscr{P}^\theta$ 是主理想. 由此可得出分圆数域 $Q(\zeta_m)$中一个重要结果:

$Q(\zeta_m)$的理想类群 C_m 是 $Z[G]$-模,其中 $G=\mathrm{Gal}(Q(\zeta_m)/Q)=\{\sigma_a:(a,m)=1\}$,而环 $Z[G]$的 Stickelberger 理想 $Z[G]\cap\left(\dfrac{\theta}{m}Z[G]\right)$把 C_m 零化.

我们在下节要介绍 Stickelberger 引理在函数域中的一个模拟. (引理的证明参见 Lang 的书[45]或 Washington 的书[57].)

复值 $g(\omega^a)$虽然不好计算,但是若把 Gauss 和定义成 P-adic 数域 Q_p 的代数闭包 $\overline{Q}_p$ 中的元素,则它可用 P-adic Gamma 函数 $\Gamma_p(z)$在有理数处的一些特殊值表达出来. 取 $\overline{Q}_p$ 中一个 p 次本原单位根(仍表成 ζ_p),则 $Q_p(\zeta_p)/Q_p$ 是 $p-1$次完全分歧扩张. 取 π 为 $Q_p(\zeta_p)$中一个素元,可以证明,$Q_p(\zeta_p)$中有唯一的 p 次本原单位

根 ζ_π，满足

$$\zeta_\pi \equiv 1 + \pi (\bmod \pi^2).$$

定义

$$\psi_\pi : \boldsymbol{F}_q \to \langle \zeta_\pi \rangle \subseteq \boldsymbol{Q}_P(\zeta_P)^*, \quad \psi_\pi(\alpha) = \zeta_\pi^{T(\alpha)},$$

这是 $\boldsymbol{F}_q$（取值于 $\overline{\boldsymbol{Q}}_P$）的加法特征，相当于复加法特征中的 ψ_1 所起的作用. 另一方面，取 $\overline{\boldsymbol{Q}}_P$ 中一个 $q-1$ 次本原单位根（仍记为 ζ_{q-1}），则 $\boldsymbol{Q}_p(\zeta_{q-1})/\boldsymbol{Q}_p$ 是 f 次不分歧扩张，并且 $\boldsymbol{Z}_p[\zeta_{q-1}]/(p) = \boldsymbol{F}_{p^f} = \boldsymbol{F}_q$. 我们也有 Teichmüller 乘法特征：

$$\omega : \boldsymbol{F}_q^* \to \langle \zeta_{q-1} \rangle \subseteq \boldsymbol{Z}_p[\zeta_{q-1}]$$

使得 $\qquad \omega(\alpha) \equiv \alpha \pmod P$ （对每个 $\alpha \in \boldsymbol{F}_q^*$）.

于是 $\boldsymbol{F}_q$ 的取值于 $\overline{\boldsymbol{Q}}_P$ 的乘法特征为 $\{\omega^a : 0 \leqslant a \leqslant q-2\}$. 我们有取值于 $\overline{\boldsymbol{Q}}_P$ 的 Gauss 和：

$$g_p(\omega^a) = g_p(\omega^a, \Psi_\pi) = -\sum_{\alpha \in \boldsymbol{F}_q^*} \omega^a(\alpha) \zeta_\pi^{T(\alpha)} \in \boldsymbol{Z}_p[\zeta_{q-1}, \zeta_p].$$

对每个正有理数 β，以 $\{\beta\}$ 表示 β 的分数部分，有以下定理：

Gross-Koblitz 定理 设 $q = p^f$，$0 \leqslant a \leqslant q-2$，$a$ 的 P-adic 展开为 $a = a_0 + a_1 p + \cdots + a_{f-1} p^{f-1}$，记 $s(a) = a_0 + a_1 + \cdots + a_{f-1}$，则

$$g_p(\omega^a) = (-1)^f \pi^{-s(a)} \prod_{i=0}^{f-1} \Gamma_p\left(1 - \left\{\frac{p^i a}{q-1}\right\}\right).$$

这个定理的证明见 Lang 的书[45].

现在介绍函数域上由 D. Goss[26]和 Thakur[54]引进的 Gamma 函数 $\Gamma_P(z)$，它是从 $\boldsymbol{Z}_p$ 到 k_P 的连续函数，这里 p 是 $k = \boldsymbol{F}_q(T)$ 的特征，而 $P = P(T)$ 为 $R = \boldsymbol{F}_q[T]$ 中首1 不可约多项式，k_P 是 k 对 P 的完备化. 记 $d = \deg P \geqslant 1$，则

$$k_P \cong \boldsymbol{F}_{q^d}((\pi)),$$

其中 π 为 k_P 中一个素元（即 $v_p(\pi) = 1$，例如可取 $\pi = P$）.

我们在 § 4.5曾介绍过 Carlitz 对于阶乘函数 $m!$ 在函数域上的模拟：

$$\Gamma_m = D_0^{\alpha_0} D_1^{\alpha_1} \cdots D_v^{\alpha_v} \in \boldsymbol{F}_q[T],$$

其中 $m = \alpha_0 + \alpha_1 q + \cdots + \alpha_v q^v$ 是非负整数 m 的 q-adic 展开，而

$D_0=1$，$D_i=[i][i-1]^q\cdots[1]^{q^{i-1}}$ $(i\geqslant 1)$，$[i]=T^{q^i}-T$.
由引理4.4.3知道

$$D_i=\prod_{\substack{A\in R_1\\ \deg A=i}} A, \tag{5.2.1}$$

式中 R_1 仍表示 $R=F_q[T]$ 中首1多项式全体. 像定义 P-adic Gamma 函数 $\Gamma_p(z)$ 一样，为了在 k_P 中收敛，我们需要把(5.2.1)式右端被 P 除尽的那些因子 A 去掉，即令

$$D_{i,P}=\prod_{\substack{A\in R_1\\ P\nmid A,\deg A=i}} A.$$

对于 $\alpha\in \mathbf{Z}_p$，设 α 的 q-adic 展开为 $\alpha=\sum\limits_{i\geqslant 0}n_iq^i$，$0\leqslant n_i\leqslant q-1$. 考虑函数

$$\prod\nolimits_P:\mathbf{Z}_p\to k_P,\ \prod\nolimits_P(\alpha)=\prod_{i\geqslant 0}(-D_{i,P})^{n_i}. \tag{5.2.2}$$

下面的引理表明(5.2.2)式右端的无穷乘积是收敛的(对于 P-adic 拓扑).

引理5.2.1 当 $i\to\infty$ 时，$-D_{i,P}\to 1$（对于 P-adic 拓扑).

证明 设 $i>d=\deg P$，令 $w=\left[\dfrac{i}{d}\right]$，则

$$\begin{aligned}D_{i,P}&=\prod_{\substack{B\in R_1\\ \deg B=i-dw}}\times\prod_{\substack{E\in R\\ \deg E<dw\\ P\nmid E}}(BP^w+E)\\ &\equiv\Big(\prod_E E\Big)^{q^{i-dw}}\pmod{P^w},\end{aligned}$$

其中 E 恰好过群 $G=(R/(P^w))^*$ 的完全代表系. 当 $2\nmid q$ 时，乘法群 G 中只有 -1 是二阶元素. 于是

$$D_{i,P}\equiv\Big(\prod_{E\in G}E\Big)^{q^{i-dw}}\equiv(-1)^{q^{i-dw}}=-1\pmod{P^w}. \tag{5.2.3}$$

当 $2\mid q$ 时，易知 $\prod\limits_{E\in G}E\equiv 1\pmod{P^w}$，从而 $D_{i,P}\equiv 1=-1\pmod{P^w}$，即(5.2.3)式也成立. 当 $i\to\infty$ 时，$w\to\infty$，而(5.2.3)式表明 $-D_{i,P}\to 1$. 证毕. ▌

从而由(5.2.2)式定义出函数：

$$\prod_P : \mathbf{Z}_p \to k_P.$$

易知这是连续函数.

定义 P-adic Gamma 函数定义为

$$\Gamma_P : \mathbf{Z}_p \to k_P, \quad \Gamma_P(z) = \Pi_P(z-1).$$

于是 Γ_P 为连续函数,并且对每个 $a \in \mathbf{Z}_p$ 有 $v_P(\Gamma_P(a))=0$. 例如,由定义可知

$$\Gamma_P(0) = \Pi_P(-1) = \left(\prod_{i \geqslant 0} D_{i,P}\right)^{q-1}$$

$$\left(\text{因为 } -1 = \sum_{i \geqslant 0}(q-1)q^i\right),$$

$$\Gamma_P(1) = \Pi_P(0) = 1,$$

$$\Gamma_P(2) = \Pi_P(1) = -D_{0,P} = -1,$$

$$\Gamma_P(q^i+1) = \Pi_P(q^i) = -D_{i,P} \quad (i \geqslant 0),$$

$$\Gamma_P(q^i) = (D_{0,P}D_{1,P}\cdots D_{i-1,P})^{q-1} = \left(\prod_{\substack{A \in R_1 \\ P \nmid A, \deg A \leqslant i-1}} A\right)^{q-1} \quad (i \geqslant 1).$$

下面要证明:事实上 $\Gamma_P(0)=(-1)^{d-1}$.

我们知道,域 $R/(P)$ 同构于 $\mathbf{F}_{q^d}$. 设 χ_0: $R/(P) \simeq \mathbf{F}_{q^d}$ 是取定的一个同构,则所有 $\mathbf{F}_q$-同构为

$$\chi_j = \chi_0^{q^j} \quad (0 \leqslant j \leqslant d-1).$$

于是

$$P(\chi_j(T)) = \chi_j(P(T)) = 0 \quad (0 \leqslant j \leqslant d-1).$$

所以 $\chi_j(T)$ $(0 \leqslant j \leqslant d-1)$ 是多项式 $P(T)$ 在 $\mathbf{F}_{q^d}$ 中的 d 个根,即 $P(T)$ 在 $\mathbf{F}_{q^d}[T]$ 中分解成 d 个一次多项式的积:

$$P(T) = \prod_{j=0}^{d-1}(T - \chi_j(T)).$$

记 $P_j = T - \chi_{1-j}(T) \in \mathbf{F}_{q^d}[T]$, 则 $P = P_1 \cdots P_d$,进而,由 $\mathbf{F}_{q^d}$ 的自同构 $\sigma(\alpha)=\alpha^q$ 诱导出域 $\mathbf{F}_{q^d}(T)$ 的自同构,使 $\sigma(T)=T$. 则

$$P_j^\sigma = T - \chi_{1-j}(T)^q = T - \chi_{1-(j+1)}(T) = P_{j-1}.$$

引理5.2.2 对于 $0 \leqslant r \leqslant d-1$,

(1) $\prod_P\left(\frac{q^r}{1-q^d}\right)\equiv -D_r \pmod P$.

(2) $\prod_P\left(\frac{q^r}{1-q^d}\right)^{q^d-1}=(-1)^{d-1}P_1^{e_r}$.

其中 $e_r=\sum_{i=0}^{d-1}(q^r-q^i)\sigma^{r-i}$.

证明 记

$$M_r=\prod_P\left(\frac{q^r}{1-q^d}\right)$$
$$=(-D_{r,P})(-D_{r+d,P})(-D_{r+2d,P})\cdots,$$
$$\mathscr{D}_{r+md}=D_{r,P}\cdot D_{r+d,P}\cdots D_{r+md,P}.$$

则
$$M_r=\lim_{m\to\infty}(-1)^{m+1}\mathscr{D}_{r+md}.$$

由于

$$D_{a,P}=\prod_{\substack{A\in R_1\\ P\nmid A,\deg A=a}}A=\prod_{\substack{A\in R_1\\ \deg A=a}}A\Bigg/\prod_{\substack{A\in R_1\\ P\mid A,\deg A=a}}A=D_a/D_{a-d}P^{q^{a-d}},$$

所以 $\mathscr{D}_{r+md}=D_{r+md}\cdot P^{-w}$(对某个正整数 w). 而

$$\mathscr{D}_{r+md}=[r+md][r-1+md]^q\cdots\frac{[md]^{q^r}}{P^{q^r}}$$
$$\cdots[r+1+(m-1)d]^{q^{d-1}}\cdot\mathscr{D}^{q^d}_{r+(m-1)d}. \tag{5.2.4}$$

这是由于$[s]=T^{q^s}-T=\prod_{\substack{P\\ \deg P\mid s}}P$. 另一方面,$T$ 是域 $K_P\cong F_{q^d}((\pi))$中的单位,即 $V_P(T)=0$. 于是

$$T=au,\ a\in F_{q^d}^*,\ u\equiv 1\pmod\pi,\ a=\chi_0(T).$$

当 $t\to\infty$时, $u^{q^t}\to 1$,所以

$$\lim_{m\to\infty}[l+md]=\lim_{m\to\infty}(au)^{q^{l+md}}-T=a_{q^l}-T.$$

由于 $T-a=T-\chi_0(T)=P_1$,作用于 σ^l,便得到 $a^{q^l}-T=-P_{1-l}$. 这就表明了

$$\lim_{m\to\infty}[l+md]=-P_{1-l}.$$

将(5.2.4)式取极限($m\to\infty$),就得到

$$M_r^{1-q^d}=-\frac{(-P_{1-r})(-P_{2-r})^q\cdots(-P_{d-r})^{q^{d-1}}}{P^{q^r}}=(-1)^{d-1}P_1^{-e_r}.$$

这就是(2)中的公式. 最后,当 $j\geqslant d$ 时,$-D_{j,P}\equiv1\pmod P$(见引理5.2.1的证明). 所以由 M_r 的定义可知

$$M_r\equiv-D_{r,P}=-D_r\pmod P.$$

这就证明了(1). 从而引理得证. ▌

作为引理5.2.2的应用,我们可以算出如下结果:

系5.2.3 $\Gamma_P(0)=(-1)^{d-1}$,其中 $d=\deg P$.

证明 $\Gamma_P(0)=\prod_P(-1)=\prod\limits_{i=0}^{\infty}(-D_{i,P})^{q-1}$

$$=(M_0M_1\cdots M_{d-1})^{q-1}.$$

由引理5.2.2可知

$$\Gamma_P(0)^{\frac{q^d-1}{q-1}}=(M_0M_1\cdots M_{d-1})^{q^d-1}=P_1^e,$$

其中

$$e=\sum_{r=0}^{d-1}e_r=\sum_{i,r=0}^{d-1}(q^r-q^i)\sigma^{r-i}$$

$$=\sum_{r=0}^{d-1}q^r\sum_{i=0}^{d-1}\sigma^{r-i}-\sum_{i=0}^{d-1}q^i\sum_{r=0}^{d-1}\sigma^{r-i}$$

$$=(1+\sigma+\cdots+\sigma^{d-1})\left(\sum_{r=0}^{d-1}q^r-\sum_{i=0}^{d-1}q^i\right)=0.$$

这就表明了 $\Gamma_P(0)^{\frac{q^d-1}{q-1}}=1$. 因此 $\Gamma_P(0)\in\boldsymbol{F}_{q^d}$. 另一方面,由引理5.2.2又知

$$\Gamma_P(0)\equiv D_0^{q-1}\cdots D_{d-1}^{q-1}\pmod P$$

$$\equiv(-1)^d\prod_{\substack{A\in k\\0\leqslant\deg A\leqslant d-1}}A\pmod P$$

$$\equiv(-1)^{d-1}\pmod P.$$

所以必然有 $\Gamma_P(0)=(-1)^{d-1}$. ▌

系5.2.4 对每个整数 i,$\Gamma_P\left(\frac{i}{q^d-1}\right)$ 均是 $k=\boldsymbol{F}_q(T)$ 上的代数元素.

证明 由于 $P_j\in\boldsymbol{F}_{q^d}[T]$,从而 $P_j(0\leqslant j\leqslant d-1)$ 均是 k 上的代

数元素. 再由引理5.2.2的(2)可知 $M_r\cdot\prod_p\left(\frac{q^r}{1-q^d}\right)$ 为 k 上的代数元素$(0\leqslant r\leqslant d-1)$. 对每个整数 i $(0\leqslant i<q^d-1)$, 令 $i=\sum_{j=0}^{d-1}a_jq^j$ 为 q-adic 展开, 则 $\prod_p\left(\frac{i}{1-q^d}\right)=\prod_{j=0}^{d-1}M_j^{a_j}$ 也是 k 上的代数元素. 最后, 设 $z\in\mathbf{Z}_p$, $z\neq-1$, 令 $z+1=a_rq^r+a_{r+1}q^{r+1}+\cdots$ 是 $z+1$ $(\neq0)$ 的 q-adic 展开, 其中 $1\leqslant a_r<q-1$, $r\geqslant0$. 则

$$z=(q-1)+(q-1)q+\cdots+(q-1)q^{r-1}$$
$$+(a_r-1)q^r+a_{r+1}q^{r+1}+\cdots.$$

所以

$$\prod_p(z+1)/\prod_p(z)=\frac{(-D_{r,p})}{\prod_{i=0}^{r-1}(-D_{i,p})^{q-1}}\in k.$$

这就表明 $\prod_p(z+1)$ 是在 k 上的代数元素 $\Leftrightarrow\prod_p(z)$ 是在 k 上的代数元素. 但是前面已证当 $0\leqslant i<q^d-1$ 时, $\prod_p\left(\frac{i}{1-q^d}\right)$ 是在 k 上的代数元素. 双向用归纳法可知对每个 $i\in\mathbf{Z}$, $\prod_p\left(\frac{i}{1-q^d}\right)$ 均是在 k 上的代数元素. 再由 $\Gamma_P(z)=\prod_P(z-1)$ 即证得系5.2.4. ▌

现在我们证明 $\Gamma_P(z)$ 具有与 $\Gamma(z)$ 和 $\Gamma_p(z)$ 类似的递推公式、函数方程和乘积公式. 这些性质可以在更一般的形式下推导出来. 为此, 我们设 $\{A_j: j=0,1,2,\cdots\}$ 是无穷多个抽象的符号. 而 G 是由这些符号生成的广义自由 Abel 群. 换句话说, G 中每个元素唯一地表示成:

$$g=\prod_{j=0}^{\infty}A_j^{a_j},$$

其中 a_j 均为整数(我们不要求 a_j 只有有限多个非零). 而群运算为

$$\left(\prod_{j\geqslant0}A_j^{a_j}\right)\left(\prod_{j\geqslant0}A_j^{b_j}\right)=\prod_{j\geqslant0}A_j^{a_j+b_j}.$$

现在对 $a\in\mathbf{Z}_p$ 令 $a=\sum_{j\geqslant 0}a_jq^j$ 为 q-adic 展开，定义映射

$$f:\mathbf{Z}_p\to G,\quad f(a)=\prod_{j\geqslant 0}A_j^{a_j}.$$

又令 $g(z)=f(z-1)$. 于是

$$g(1)=f(0)=1,\ g(0)=f(-1)=\prod_{j\geqslant 0}A_j^{q-1}.$$

特别取 $A_j=-D_j$，则

$$f(a)=\prod\nolimits_p(a),\ g(a)=\Gamma_p(a).$$

引理5.2.5 设 $z\in\mathbf{Z}_p$.

(1) 递推公式　若 $z\neq 0$, $\mathrm{ord}_q(z)=m$ ($\geqslant 0$)(这意味着 $z\in q^m\mathbf{Z}_p$，但是 $z\notin q^{m+1}\mathbf{Z}_p$). 则

$$\frac{g(z+1)}{g(z)}=\frac{A_m}{(A_0\cdots A_{m-1})^{q-1}}\quad\left(\text{当 } m=0 \text{ 时}, \frac{g(z+1)}{g(z)}=A_0\right).$$

(2) 函数方程 $g(z)\cdot g(1-z)=g(0)$.

(3) 若 n 为正整数，并且 $(n,p)=1$，则(乘积公式)

$$g(z)g\left(z+\frac{1}{n}\right)\cdots g\left(z+\frac{n-1}{n}\right)=g(0)^{\frac{n-1}{2}}g(nz).$$

(注意，当 $2|n$ 时，必然 $2\nmid q$. 这时 $g(0)^{\frac{1}{2}}$ 是指 $\prod_{j\geqslant 0}A_j^{\frac{q-1}{2}}$.)

证明 (1) 参见系5.2.4的证明.

(2) 若 $z-1=\sum_{j=0}^{\infty}n_jq^j$ 为 q-adic 展开，则

$$-1-(z-1)=\sum_{j=0}^{\infty}(q-1-n_j)q^j.$$

于是

$$\begin{aligned}g(z)g(1-z)&=f(z-1)\cdot f(-1-(z-1))\\&=\prod_{j\geqslant 0}A_j^{q-1}=g(0).\end{aligned}$$

(3) 由 $(n,p)=1$ 可知 $\mathrm{ord}_q(z)=\mathrm{ord}_q(nz)$. 由(1)可知

$$\frac{g(z)}{g(z+1)}=\frac{g(nz)}{g(nz+1)}.$$

从而

$$\frac{g(z)g\left(z+\frac{1}{n}\right)\cdots g\left(z+\frac{n-1}{n}\right)}{g(nz)}$$

$$\times\frac{g(nz+1)}{g\left(z+\frac{1}{n}\right)g\left(z+\frac{2}{n}\right)\cdots g\left(z+\frac{n-1}{n}\right)g(z+1)}$$

$$=\frac{g(z)\cdot g(nz+1)}{g(z+1)\cdot g(nz)}=1.$$

这表明：若乘积公式对 z 成立，则对 $z+\frac{1}{n}$ 也成立. 但是当 $z=\frac{1}{n}$ 时，由函数方程(2)可知：

$$\frac{g\left(\frac{1}{n}\right)g\left(\frac{2}{n}\right)\cdots g\left(\frac{n-1}{n}\right)g(1)}{g(1)}=g\left(\frac{1}{n}\right)g\left(\frac{2}{n}\right)\cdots g\left(\frac{n-1}{n}\right)$$

$$=g(0)^{\frac{n-1}{2}}.$$

即 $z=\frac{1}{n}$ 时乘积公式成立. 于是对 $z=\frac{2}{n},\frac{3}{n},\cdots$，乘积公式也成立. 特别地，当 z 为任何正整数时，乘积公式成立. 由于正整数集合是 $\mathbf{Z}_p$ 的稠密子集，而 $\Gamma_P(z)$ 是连续函数，所以对每个 $z\in\mathbf{Z}_p$，乘积公式均成立. ∎

定理5.2.6 设 $z\in\mathbf{Z}_p$，$d=\deg P$.

(1) 若 $z\neq0$. $\mathrm{ord}_q(z)=m(\geqslant0)$，则

$$\frac{\Gamma_P(z+1)}{\Gamma_P(z)}=-\frac{D_{m,P}}{(D_{0,P}D_{1,P}\cdots D_{m-1,P})^{q-1}}.$$

特别是当 $\mathrm{ord}_q(z)=0$时，$\Gamma_P(z+1)=-\Gamma_P(z)$.

(2) $\Gamma_P(z)\Gamma_P(1-z)=(-1)^{d-1}$.

(3) 若 n 为正整数，并且$(n,p)=1$，则

$$\prod_{i=0}^{n-1}\Gamma_P\left(z+\frac{i}{n}\right)=(-1)^{\frac{(n-1)(d-1)}{2}}\Gamma_P(nz).$$

当$2\nmid q$ 并且$2\nmid(n-1)(d-1)$时，$(-1)^{\frac{(n-1)(d-1)}{2}}=(-1)^{\frac{1}{2}}(\in\boldsymbol{F}_q^*)$ 的符号由

$$(-1)^{\frac{d-1}{2}}=\Gamma_P(0)^{\frac{1}{2}}=\prod_{j\geqslant0}(-D_{j,P})^{\frac{q-1}{2}}=(M_0M_1\cdots M_{d-1})^{\frac{q-1}{2}}$$

$$\equiv (D_0 \cdots D_r)^{\frac{q-1}{2}} \pmod P$$

$$\equiv \Big(\prod_{\substack{A\in R_1 \\ \deg A < d}} A\Big)^{\frac{q-1}{2}} \pmod P$$

所决定.

证明 由引理5.2.5和系5.2.3即得. ∎

§5.3 高 斯 和

本节中介绍 Thakur[55]发展的函数域上的高斯和. 仍记

$$k = \boldsymbol{F}_q(T),\ R = \boldsymbol{F}_q[T],\ K = k(\Lambda_P),$$

其中 P 是 R 中首1不可约多项式, $\deg P = h \geqslant 1$. 又记 $q' = q^h$, 而

$$k' = \boldsymbol{F}_{q'}(T),\quad K' = k'K = k'(\Lambda_P) = \boldsymbol{F}_{q'}K$$

分别是 k 和 K 的常数域扩张. 于是有域的扩张和 P 在扩域中的分解(图5.1.,5.2):

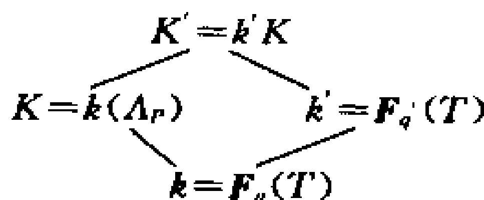


图 5.1

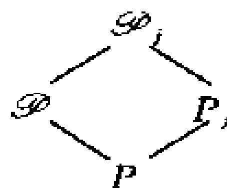


图 5.2

P 在 k' 中分解成 h 个一次多项式之积:

$$P = P_0 P_1 \cdots P_{h-1},$$

其中 $P_j = T - \chi_{1-j}(T)$, $\chi_j\,(0 \leqslant j \leqslant h-1)$ 是引理5.2.2前面所叙述的同构

$$R/(P) \simeq \boldsymbol{F}_{q^h},\ \chi_j = \chi_0^{q^j}.$$

而 $P = P_0 P_1 \cdots P_{h-1}$, $\mathscr{P} = \mathscr{P}_0 \mathscr{P}_1 \cdots \mathscr{P}_{h-1}$, $P = \mathscr{P}^{q^h-1}$, $P_j = \mathscr{P}_j^{q^h-1}$. 由于 K 和 k' 是 k 的线性无缘扩张, 从而有

$$\mathrm{Gal}(K'/k) = \mathrm{Gal}(K/k) \times \mathrm{Gal}(k'/k),$$

其中 $\mathrm{Gal}(K/k) = \{\sigma_A \mid A \in (R/(P))^*\}$, $\sigma_A(\lambda) = \lambda^A$, λ 是任意取定的一个本原 P-torsion 元素. 而 $\mathrm{Gal}(k'/k) = \langle\sigma\rangle$, 其中对每个

$\alpha\in F_{q'}$，$\sigma(\alpha)=\alpha^q$. 而 σ 和 σ_A 在 K 和 k' 上分别是恒等映射. 于是

$$P_j^\sigma = (T-\chi_{1-j}(T))^\sigma = T-\chi_{1-j}^q(T)$$
$$= T-\chi_{1-(j-1)}(T) = P_{j-1}.$$

对于 R-模同构

$$\psi: R/(P) \to \Lambda_P,\quad \psi(A(\mathrm{mod}\ P)) = \bar{\lambda}^P,$$

Thakur 定义了如下的高斯和：

$$g_j = -\sum_{A\in(R/(P))^*}\chi_j(A^{-1})\psi(A)\in K'\quad(0\leqslant j\leqslant h-1).$$

我们规定 $g_{j+h}=g_j$. 下面是 g_j 的基本性质：

引理5.3.1　(1) $\psi(z)=\sum_{j=0}^{h-1}g_j\chi_j(z)$；

(2) $g_j^\sigma=g_{j+1}, g_j^{\sigma_A}=\chi_j(A)g_j\quad(A\in(R/(P))^*)$，

$$g_j\neq 0\quad(0\leqslant j\leqslant h-1);$$

(3) $\left(\prod_{j=0}^{h-1}g_j\right)^{q-1}=(-1)^hP$.

证明　(1) $z=0$时，等式显然成立. 对于 $z\in(R/(P))^*$，则等式右端为

$$\sum_{j=0}^{h-1}g_j\chi_j(z) = -\sum_{j=0}^{h-1}\chi_j(z)\sum_{A\in(R/(P))^*}\chi_j(A^{-1})\psi(A)$$
$$= -\sum_{A\in(R/(P))^*}\psi(A)\sum_{j=0}^{h-1}\chi_j(zA^{-1})$$
$$= -\psi(z)\sum_{B\in(R/(P))^*}\psi(B^{-1})\sum_{j=0}^{h-1}\chi_j(B)$$

(其中令 $B=zA^{-1}$)

$$= -\psi(z)\sum_{a\in F_q^*}a\sum_{\substack{B\in(R/(P))^*\\ Tr(\chi_0(B))=a}}\psi(B^{-1})$$

(其中 $Tr(\alpha)=\sum_{i=0}^{h-1}\alpha^{q^i}\in F_q$)

$$= -\psi(z)\sum_{a\in F_q^*}a\sum_{\substack{A\in(R/(P))^*\\ Tr(\chi_0(A))=1}}a^{-1}\psi(A^{-1})$$

$$
\begin{aligned}
&(\text{令 } B = aA) \\
&= -\psi(z) \sum_{\substack{A\in (R/(P))^* \\ Tr(\chi_0(A))=1}} \psi(A^{-1}) \sum_{a\in F_q^*} 1 \\
&= \psi(z) \sum_{\substack{A\in (R/(P))^* \\ Tr(\chi_0(A))=1}} \psi(A^{-1}) = \psi(z)\psi(\sum A^{-1}).
\end{aligned}
$$

(5.3.1)

若 $\chi_0(A)=a\in F_{q'}$，$Tr(a)=1$，则 a 是$1-x-x^q-x^{q^2}-\cdots-x^{q^{h-1}}$的根，于是 a^{-1}为 $x^{q^{h-1}}-x^{q^{h-2}}-x^{q^{h-3}}-\cdots-1$的根，从而 A^{-1}也是如此，所有这些 A^{-1}的和为1. 因此(5.3.1)式右端为 $\psi(z)\psi(1)=\psi(z)$. 这就证明了(1).

(2) 由 $\chi_j^q=\chi_{j+1}$，$\psi(B)^{\sigma_A}=\lambda^{BA}=\psi(BA)$可知

$$
g_j^q = -\sum_A \chi_j^q(A^{-1})\psi(A) = -\sum_A \chi_{j+1}(A^{-1})\psi(A) = g_{j+1},
$$

$$
\begin{aligned}
g_j^{\sigma_A} &= -\sum_B \chi_j(B^{-1})\psi(B)^{\sigma_A} = -\sum_B \chi_j(B^{-1})\psi(AB) \\
&= -\sum_C \chi_j(A)\chi(C^{-1})\psi(C) = \chi_j(A)g_j.
\end{aligned}
$$

最后，若对某个 $j(0\leqslant j\leqslant h-1)$，$g_j=0$，则由 $g_j^q=g_{j+1}$可知，对所有$0\leqslant j\leqslant h-1$，$g_j=0$，由(1)知 $\psi(z)=0$(对所有 $z\in R/(P)$)，但这是不可能的，因为 $\psi:R/(P)\to\Lambda_P$ 是 R-模同构. 所以对所有$0\leqslant j\leqslant h-1$，有 $g_j\neq 0$.

(3) 由于 ψ 是 R-模同构，所以有 $\psi(Tz)=T\psi(z)+\psi(z)^q$. 于是当 $P\neq T$ 时，

$$
\begin{aligned}
g_j\chi_j(T) &= -\sum_{A\in (R/(P))^*} \chi_j(A^{-1}T)\psi(A) \\
&= -\sum_B \chi_j(B^{-1})\psi(TB) \quad (\text{令 } A^{-1}T = B^{-1}) \\
&= -\sum_B \chi_j(B^{-1})(T\psi(B) + \psi(B)^q) \\
&= Tg_j + g_{j-1}^q.
\end{aligned}
$$

由于 $g_j\neq 0$，从而有

$$\frac{g_{j-1}^{q}}{g_j}=\chi_j(T)-T=-P_{1-j},\tag{5.3.2}$$

$$(g_0\cdots g_{h-1})^{q-1}=\prod_{j=0}^{h-1}(g_{j-1}^{q}/g_j)$$
$$=(-1)^hP_0P_1\cdots P_{h-1}=(-1)^hP.$$

若 $P=T$，则 $h=1$，$k'=k$，本原 P-torsion 元素 $\bar{\lambda}$ 是方程 $u^T/u=T+u^{q-1}$ 的根，因此 $\bar{\lambda}^{q-1}=-T$. 所以

$$g_0=-\sum_{a\in F_q^*}\chi_0(a^{-1})\psi(a)=-\sum_{a\in F_q^*}a^{-1}a\bar{\lambda}=\bar{\lambda},$$

即 $g_0^{q-1}=\bar{\lambda}^{q-1}=-T=-P$. ∎

引理5.3.2　设 k_P 是 $k=\boldsymbol{F}_q(T)$ 对于素除子 P 的局部域，$N=q^h-1$. 则存在 $\lambda\in k_P(\bar{\lambda})$，使得

$$\lambda^N=-P,\lambda\equiv\bar{\lambda}\pmod{\bar{\lambda}^2}.$$

证明　局部域扩张 $k_P(\bar{\lambda})/k_P$ 是 N 次全分歧扩张. 由于 $\boldsymbol{F}_{q^h}\subseteq k_P\cong\boldsymbol{F}_{q^h}((P))$，所以这也是 Kummer 扩张. 即

$$k_P(\bar{\lambda})=k_P((-\pi)^{1/N}),$$

其中 $\pi\in k_P$，而 $\bar{\lambda}$ 和 $(-\pi)^{1/N}$ 均是 $k_P(\bar{\lambda})$ 中的素元(由于 $(-\pi)^{1/N}$ 和 $\bar{\lambda}$ 在 k_P 上的极小多项式分别为 $u^N+\pi$ 和 $u^P/u=u^N+\cdots+P$，所以 $(-\pi)^{1/N}$ 和 $\bar{\lambda}$ 对于扩张 $k_P(\bar{\lambda})/k_P$ 的范数分别为 π 和 P). 这表明 $\frac{(-\pi)^{1/N}}{\bar{\lambda}}$ 为 $k_P(\bar{\lambda})$ 中的单位. 于是

$$(-\pi)^{1/N}\equiv a\bar{\lambda}\pmod{\bar{\lambda}^2},$$

其中 $a\in\boldsymbol{F}_q^*$. 于是

$$\frac{\pi}{P}\equiv N_{k_P(\bar{\lambda})/k_P}\left(\frac{(-\pi)^{\frac{1}{N}}}{\bar{\lambda}}\right)\equiv N(a)=a^N\equiv1\pmod{\bar{\lambda}}.$$

由 Hensel 引理可知 $\left(\frac{\pi}{P}\right)^{\frac{1}{N}}\in k_P(\bar{\lambda})$. 但是 $(-\pi)^{\frac{1}{N}}\in k_P(\bar{\lambda})$，从而 $(-P)^{\frac{1}{N}}\in k_P(\bar{\lambda})$，即 $(-P)^{\frac{1}{N}}$ 为 $k_P(\bar{\lambda})$ 中的素元. 于是 $(-P)^{\frac{1}{N}}\equiv a\bar{\lambda}\pmod{\bar{\lambda}^2}$，其中 $a\in\boldsymbol{F}_q^*$，取 $\lambda=a^{-1}(-P)^{\frac{1}{N}}$ 即可. ∎

现在可以证明上节所述关于高斯和的 Stickelberger 定理在

函数域的模拟.

定理5.3.3 (1) 令 $d_0=1$, $d_j=-P_{1-j}d_{j-1}^q$ $(1\leqslant j\leqslant h-1)$, $\lambda\in k_P(\lambda)\subseteq K'_{\mathscr{P}_1}$. 则

$$g_j/\lambda^{q^j}\equiv d_j^{-1}\pmod{\mathscr{P}_1}\quad(0\leqslant j\leqslant h-1).$$

(2) 高斯和 g_j 在 K' 中的素理想分解为

$$(g_j)=\mathscr{P}_{1-j}\mathscr{P}_{2-j}^{q}\cdots\mathscr{P}_{h-j}^{q^{h-1}}\quad(0\leqslant j\leqslant h-1).$$

(3) 设 v 是 k 中无限素除子 v_∞ 到 K' 的一个扩充,则

$$v(g_j)=-\frac{1}{q-1}.$$

证明 (1) 先证 $j=0$ 的情形:

$$\begin{aligned}g_0&=-\sum_{A\in(R/(P))^*}\chi_0(A^{-1})\psi(A)=-\sum_A\chi_0(A^{-1})\bar{\lambda}^A\\&\equiv-\sum_A\chi_0(A^{-1})A\bar{\lambda}\pmod{\bar{\lambda}^2}\\&\equiv-\sum_A A^{-1}\cdot A\bar{\lambda}\equiv\bar{\lambda}\equiv\lambda\pmod{\mathscr{P}_1^2}.\end{aligned}$$

于是 $g_0/\lambda\equiv1\pmod{\mathscr{P}_1}$,即 $j=0$ 时成立. 现在设 $1\leqslant j\leqslant h-1$,并且

$$g_{j-1}/\lambda^{q^{j-1}}\equiv\frac{1}{d_{j-1}}\pmod{\mathscr{P}_1},$$

则由(5.3.2)式知(注意 P_{1-j} 和 $\mathscr{P}_1$ 互素):

$$\frac{g_j}{\lambda^{q^j}}=\frac{-g_{j-1}^q}{P_{1-j}\lambda^{q^j}}\equiv\frac{1}{-P_{1-j}d_{j-1}^q}\equiv\frac{1}{d_j}\pmod{\mathscr{P}_1}.$$

(1) 得证.

(2) 由定理5.3.1的(3)可知理想 (g_j) 在 K' 中的素因子只能为 $\mathscr{P}_j$ $(0\leqslant j\leqslant h-1)$. 本定理的(1)表明了 $v_{\mathscr{P}_1}(g_j)=q^j$ $(0\leqslant j\leqslant h-1)$,因为 d_j 和 $\mathscr{P}_1$ 互素,于是当 $1\leqslant j\leqslant h-1$ 时,

$$\begin{aligned}q^j&=v_{\sigma(\mathscr{P}_1)}(\sigma(g^j))=v_{\mathscr{P}_0}(g_{j+1})=v_{\mathscr{P}_0}(P_{-j}^{-1}g_j^q)\\&=v_{\mathscr{P}_0}(g_j^q).\end{aligned}$$

这表明 $v_{\mathscr{P}_0}(g_j)=q^{j-1}$,从而 $v_{\mathscr{P}_j}(g_0)=q^{j-1}$ $(1\leqslant j\leqslant h-1)$. 当 $j=0$ 时,

$1 = v_{\mathscr{P}_1}(g_0) = v_{\mathscr{P}_0}(g_1) = v_{\mathscr{P}_0}(P_0^{-1}g_0^q) = qv_{\mathscr{P}_0}(g_0) - (q^h - 1)$，所以 $v_{\mathscr{P}_0}(g_0)=q^{h-1}$. 于是 $(g_0)=\mathscr{P}_1\mathscr{P}_2^q\cdots\mathscr{P}_{h-1}^{q^{h-2}}\mathscr{P}_0^{q^{h-1}}$. 将此式作用于 σ^j，就得到

$$(g_j) = \mathscr{P}_{1-j}\mathscr{P}_{2-j}^q\cdots\mathscr{P}_{h-j}^{q^{h-1}}.$$

(2)得证.

(3) 由(2)知 $\left(g_j^{q^h-1}\right) = \left(P_{1-j}P_{2-j}^q\cdots P_{h-j}^{q^{h-1}}\right)$. 另一方面，由 $\sigma_A(g_j) = \chi_j(A)g_j$，可知 $\sigma_A\left(g_j^{q^h-1}\right) = g_j^{q^h-1}$ (对每个 $A\in(R/(P))^*$). 这表明 $g_j^{q^h-1}\in k'=\boldsymbol{F}_{q^h}(T)$. 因此上式是 k' 中理想的分解式. 于是 $g_j^{q^h-1}=aP_{1-j}P_{2-j}^q\cdots P_{h-j}^{q^{h-1}}$，其中 $a\in\boldsymbol{F}_{q^h}^*$. 所以

$$v(g_j) = \frac{1}{q^h-1}\sum_{i=1}^{h}v_\infty(P_{i-j})^{q^{i-1}} = \frac{-1}{q^h-1}\sum_{i=0}^{h-1}q^i = -\frac{1}{q-1}.$$

(3)得证. ▌

最后我们证明上节的 Gross-Koblitz 公式在函数域上的模拟.

定理5.3.4　设 $\Pi_P:\boldsymbol{Z}_p\to k_P$ 是上节定义的连续函数. 则有 $K'_{\mathscr{P}_1}$ 中的等式

$$g_j = -\lambda^{q^j}/\Pi_P\left(\frac{q^j}{1-q^h}\right)\quad(0\leqslant j\leqslant h-1).\qquad(5.3.3)$$

证明　引理5.2.2表明

$$v_{\mathscr{P}_1}\left(\Pi_P\left(\frac{q^j}{1-q^h}\right)\right) = 0,\quad v_{\mathscr{P}_1}(\lambda^{q^j}) = q^j,$$

$$v_{\mathscr{P}_1}(g_j) = q^j\quad(\text{定理 }5.3.3).$$

所以(5.3.3)式两端的 $\mathscr{P}_1$-adic 赋值相等. 我们只需再证明

$$g_j/\lambda^{q^j} \equiv \frac{-1}{\Pi_P\left(\frac{q^j}{1-q^h}\right)}\pmod{\mathscr{P}_1}\quad(0\leqslant j\leqslant h-1)\qquad(5.3.4)$$

即可. 但是

$$\frac{g_j}{\lambda^{q^j}} \equiv \frac{1}{d_j}\pmod{\mathscr{P}_1}\ (\text{定理 }5.3.3),\qquad(5.3.5)$$

$$\Pi_p\left(\frac{q^j}{1-q^{h-1}}\right) \equiv -D_j \pmod{\mathscr{P}_1} \text{ (引理 5.2.2)}. \tag{5.3.6}$$

而由 d_j 的定义知道

$$d_j = (-P_{h-j+1})(-P_{h-j+2})^q \cdots (-P_h)^{q^{j-1}}.$$

由 $T-\chi_0(T)=P_1\equiv 0 \pmod{\mathscr{P}_1}$，即 $\chi_0(T)\equiv T \pmod{\mathscr{P}_1}$，从而

$$\begin{aligned} -P_j &= \chi_{1-j}(T) - T = \chi_0(T)^{q^{1-j}} - T \\ &\equiv T^{h-j+1} - T = [h-j+1] \pmod{\mathscr{P}_1}. \end{aligned}$$

这表明

$$d_j \equiv [j][j-1]^q \cdots [1]^{q^{j-1}} = D_j \pmod{\mathscr{P}_1}.$$

再由(5.3.5)和(5.3.6)式即得(5.3.4)式. ▌

§5.4 幂 和 $S_i(k)$

在第 4 章研究分圆函数域类数整除性时，我们引进了 $\boldsymbol{F}_q[T]$ 中的 Bernoulli-Goss 多项式(定义4.1.4)

$$\beta_k(T) = \begin{cases} \displaystyle\sum_{i=0}^{k/(q-1)} S_i(k), & \text{若} (q-1) \nmid k \geqslant 1; \\ \displaystyle -\sum_{i=0}^{k/(q-1)} iS_i(k), & \text{若} (q-1) \mid k. \end{cases}$$

其中

$$S_i(k) = \sum_{\substack{A\in R_1 \\ \deg A = i}} A^k \in \boldsymbol{F}_q[T].$$

式中 R_1 表示 $\boldsymbol{F}_q[T]$ 中全体首1多项式组成的集合. 本节介绍 Gekeler[18]的关于 $S_i(k)$的若干结果. 主要问题是决定多项式$S_i(k)$的次数以及它的确切值.

首先我们有 $S_0(k)=1$，而当 $i\geqslant 1$时 $S_i(0)=0$. 其次，和 $\beta_k(T)$ 一样有递推公式，对于 $i\geqslant 1, k\geqslant 1$，有

$$S_i(k) = \sum_{\substack{B\in R_1 \\ \deg B = i-1}} \sum_{a\in \boldsymbol{F}_q} (TB+a)^k = \sum_{j=0}^{k} \binom{k}{j} T^j \sum_B B^j \sum_a a^{k-j}.$$

当$0<s\equiv 0 \pmod{q-1}$时$\sum_{\alpha}\alpha^s=-1$. 否则，$\sum_{\alpha}\alpha^s=0$. 因此

$$S_i(k)=-\sum_{\substack{j=0\\ j\equiv k(\bmod q-1)}}^{k-1}\binom{k}{j}T^jS_{i-1}(j) \qquad (5.4.1)$$

设 p 是 q 的素因子，对于 $k\geqslant 0$，以 $k=\sum k_s q^s$ 和 $k=\sum k_{s,p}p^s$ 分别表示 k 的 q-adic 展开和 P-adic 展开，$l(k)=\sum k_s$ 和 $l_p(k)=\sum_s k_{s,p}$分别为这两种展开的数字和，则 Lucas 定理可以表示成：

$$\binom{k}{j}\equiv\prod_s\binom{k_{s,p}}{j_{s,p}}\equiv\prod_s\binom{k_s}{j_s} \pmod{p}.$$

因此有

$$\begin{aligned}\binom{k}{j}\neq 0\ (\text{在 } F_q \text{ 中}) &\Leftrightarrow \text{对每个 } s\geqslant 0, j_{s,p}\leqslant k_{s,p}\\ &\Leftrightarrow l_p(k)=l_p(j)+l_p(k-j)\\ &\Rightarrow \text{对每个 } s\geqslant 0, j_s\leqslant k_s\\ &\Rightarrow l(j)\leqslant l(k).\end{aligned} \qquad (5.4.2)$$

定义5.4.1 在集合 $N=\{0,1,2,\cdots\}$上定义如下的关系：$j\Delta k$当且仅当以下三个条件成立：

(i) $j<k$；

(ii) $j\equiv k \pmod{q-1}$；

(iii) $\binom{k}{j}\not\equiv 0 \pmod{p}$.

由于 $l(j)\equiv j \pmod{q-1}$，可知 $j\Delta k\Rightarrow l(j)\leqslant l(k)-q+1$. 又由于有$\binom{r}{s}\binom{s}{t}=\binom{r}{t}\binom{r-t}{r-s}$，可知关系 Δ 是传递的，即由 $j\Delta k$ 和 $k\Delta i$ 可推出 $j\Delta i$.

每个 $k\in N$ 可唯一地表示成

$$k=\sum_{1\leqslant s\leqslant l(k)}q^{e_s}, \qquad (5.4.3)$$

其中 $e_s\leqslant e_{s+1}$（对$1\leqslant s\leqslant l(k)-1$）并且 $e_s<e_{s+q}$（对$1\leqslant s\leqslant l(k)-q$）. 如果 $k=\sum k_s q^s$ 是 k 的 q-adic 展开，则表达式(5.4.3)即是依

次把每个 $k_s q^s$ $(1\leqslant k_s\leqslant q-1)$分解成 k_s 个 q^s 而得到的.

定义 5.4.2 令 $\rho(-\infty)=-\infty$, $\rho^0(k)=k$, $\rho^i(k)=\rho(\rho^{i-1}(k))$,其中对每个 $k\in N$,令

$$\rho(k)=\begin{cases} k-\sum\limits_{1\leqslant s\leqslant q-1} q^{r_s}, & \text{如果 } l(k)\geqslant q-1; \\ -\infty, & \text{如果 } l(k)<q-1. \end{cases}$$

例 对于 $q=3$, $k=71=2+2\cdot 3+3^2+2\cdot 3^3$, 则

$$\rho(k)=69,\ \rho^2(k)=63,\ \rho^3(k)=27,\ \rho^i(k)=-\infty\ (i\geqslant 4).$$

引理5.4.3 (1) 若 $j\leqslant k$, $l(j)\leqslant l(k)$, 则 $\rho(j)\leqslant\rho(k)$.

(2) 若 $j\Delta k$,则对每个 $s\geqslant 0$, $\rho^s(j)\leqslant\rho^{s+1}(k)$.

证明 (1) 由 ρ 的定义可直接得出.

(2) 由关系 Δ 和映射 ρ 的定义可知命题对 $s=0$成立,即若 $j\Delta k$,则 $j\leqslant\rho(k)$. 现在设 $s\geqslant 1$,并且 $\rho^{s-1}(j)\leqslant\rho^s(k)$. 由 Δ 的定义和(5.4.2)式可知 $l(\rho^{s-1}(j))\leqslant l(\rho^s(k))$. 再由(1)便知 $\rho^s(j)\leqslant\rho^{s+1}(k)$. 这就归纳证明了(2) 对每个 $s\geqslant 0$均成立. ▌

现在我们可以决定多项式 $S_i(k)$的次数(注意 $\deg(0)=-\infty$).

定理5.4.4 设 $i,k\geqslant 1$. 规定对 $a\in N$, $(-\infty)+a=(-\infty)+(-\infty)=-\infty$. 则

(1) $\deg S_i(k)\leqslant\rho(k)+\rho^3(k)+\cdots+\rho^i(k)$,进而,如果

$$\binom{k}{\rho^s(k)}\not\equiv 0 \pmod{p}\quad (0\leqslant s\leqslant i), \tag{5.4.4}$$

则 $\deg S_i(k)=\sum\limits_{\lambda=1}^{i}\rho^\lambda(k)$.

(2) (Carlitz[4]的引理4.2) $S_i(k)\neq 0$当且仅当 k 可以表示成

$$k=m_0+m_1+\cdots+m_i, \tag{5.4.5}$$

其中 m_i 满足条件:令 $m_j=\sum\limits_{\lambda} m_{j,\lambda}p^\lambda$ 是 m_j 的 p-adic 展开,则

$$m_0\geqslant 0,\ (q-1)\mid m_j\geqslant 1\quad (1\leqslant j\leqslant i),$$

$$\sum_{j=0}^{i} m_{j,\lambda}\leqslant p-1\quad (\text{对每个 } \lambda\geqslant 0). \tag{5.4.6}$$

并且当满足条件(5.4.6)的分解式(5.4.5)存在时，有

$$\deg S_i(k) = \mathrm{Max}\{im_0 + (i-1)m_1 + \cdots + m_{i-1}\},$$

其中最大值在满足(5.4.5)和(5.4.6)的唯一的一组$\{m_0, m_1, \cdots, m_i\}$处达到.

证明　(1) 我们对 i 用归纳法：由递推关系(5.4.1)可知 $\deg S_i(k) \leqslant \rho(k)$. 即(1) 对于 $i=1$成立. 现设(1)对 $i-1$成立($i \geqslant 2$). 由递推关系(5.4.1)可知

$$\begin{aligned}\deg S_i(k) &\leqslant \sup_{j\Delta k}\{j + \deg S_{i-1}(j)\}\\ &\leqslant \sup_{j\Delta k}\{j + \rho(j) + \rho^2(j) + \cdots + \rho^{i-1}(j)\}\\ &\quad \text{(由归纳假设)}\\ &\leqslant \rho(k) + \rho^2(k) + \rho^3(k) + \cdots + \rho^i(k)\\ &\quad \text{(引理 5.4.3 的(2))}.\end{aligned}$$

所以对每个 $i \geqslant 1$，有 $\deg S_i(k) \leqslant \sum_{\lambda=1}^{i}\rho^\lambda(k)$. 进而若条件(5.4.4)成立，则对每个$0 \leqslant s \leqslant i$，$\rho^s(k)$为满足

$$j = j_s \Delta j_{s-1} \Delta j_{s-2} \Delta \cdots \Delta j_1 \Delta k$$

的 j 的唯一最大值. 再由递推关系(5.4.1)即知

$$\deg S_i(k) = \sum_{\lambda=1}^{i}\rho^\lambda(k).$$

(2) 可以与(1)一样类似地证得. ▌

例　设 $q=4$. 我们来计算 $\deg S_1(98)$. 由于$98 = 2 + 2 \cdot 4^2 + 4^3$，上述定理的(1)给出 $\deg S_1(98) \leqslant \rho(98) = 4^2 + 4^3 = 80$. 另一方面满足条件(5.4.6)的分解式$98 = m_0 + m_1$有$(m_0, m_1) = (2, 2^5 + 2^6) = (2, 96)$和$(m_0, m_1) = (2^5, 2 + 2^6) = (32, 66)$. 由上述定理的(2)给出$\deg S_1(98) = \mathrm{Max}\{m_0\} = 32$.

定理5.4.4有许多具体的推论：

系5.4.5　设 $i, k \geqslant 1$，p 为 q 的素因子. 对于 $F_q[T]$中的多项式 $S_i(k)$，我们有

(1) 若 $q = p^t$，则当 $i > l_p(k)/t(p-1)$时，$S_i(k) = 0$.

(2) 若 $q=p$，则 $S_i(k)=0 \Leftrightarrow i>l(k)/(q-1)$. 并且当 $l(k) \geqslant i(q-1)$时，$\deg S_i(k)=\rho(k)+\rho^2(k)+\cdots+\rho^i(k)$.

(3) 若 $k<q^i-1$，则 $S_i(k)=0$.

(4) 若 $i>l(k)/(q-1)$，则 $S_i(k)=0$.

证明 先证(4)，这是由于 $l(\rho^{i-1}(k))\leqslant l(k)-(i-1)(q-1)<q-1$. 所以 $\rho^i(k)=-\infty$，即 $S_i(k)=0$.

(3) 由(4)即得. 因为当 $k<q^i-1$时，$l(k)<i(q-1)$.

(1) 如果分解式(5.4.5)满足条件(5.4.6)，则

$$l_p(m_j)\geqslant t(p-1) \quad (1\leqslant j\leqslant i),$$

$$l_p(k)=l_p(m_0)+l_p(m_1)+\cdots+l_p(m_i)\geqslant it(p-1).$$

所以当 $i>l_p(k)/t(p-1)$时，$S_i(k)=0$.

(2) 若 $q=p$，则 $S_i(k)\neq 0 \Leftrightarrow$ 满足条件(5.4.6)的分解式(5.4.5)存在 $\Leftrightarrow l(k)\geqslant i(q-1) \Rightarrow \deg S_i(k)=\sum_{\lambda=1}^{i}\rho^\lambda(k)$. ∎

以上我们决定了多项式 $\deg S_i(k)$的次数. 现在对于某些特殊的 k，计算多项式 $S_i(k)$的具体表达式. 对每个 $i\geqslant 0$，令

$$R(i)=\{A\in R=\boldsymbol{F}_q[T]:\deg A<i\},$$

$$e_i(z)=\prod_{A\in R(i)}(z-A).$$

则由引理4.4.3算出

$$e_i(z)=\sum_{k=0}^{i}(-1)^{i-k}\begin{bmatrix} i \\ k \end{bmatrix} z^{q^k}, \tag{5.4.7}$$

其中

$$\begin{bmatrix} i \\ k \end{bmatrix}=D_i/D_kL_{i-k}^{q^k}.$$

现在定义

$$[k]_m=[k][k-1]^q\cdots[k-m+1]^{q^{m-1}}=\frac{D_k}{D_{k-m}^{q^m}},$$

$$\begin{Bmatrix} m \\ j \end{Bmatrix}=\frac{D_m}{D_jD_{m-j}^{q^j}}=\frac{[m]_j}{D_j}.$$

引理5.4.6 $z^{q^k}=\sum_{j=0}^{k}\begin{Bmatrix} m \\ j \end{Bmatrix}e_j(z)$.

证明 令 $z^{q^k}=\sum_{j=0}^{k}b_j e_j(z)$. 由引理5.1.2可知

$$b_j=\frac{\Delta^{(j)}(z^{q^k})}{D_j}\bigg|_{z=1}=\prod_{\lambda=0}^{j-1}(T^{q^k}-T^{q^\lambda})/D_j \quad (\text{引理 } 5.1.1)$$

$$=[k][k-1]^q\cdots[k-j+1]^{q^{j-1}}/D_j=\frac{[k]_j}{D_j}=\begin{Bmatrix}k\\j\end{Bmatrix}.$$ ▌

现在设 $k=a_0+a_1q+\cdots+a_tq^t$ 为 k 的 q-adic 展开. 回顾 §5.1 中定义的 Carlitz 函数

$$G_k(z)=\prod_j e_j(z)^{a_j}.$$

引理5.4.7 (Carlitz[3])

$$\sum_{\substack{A\in R_1\\ \deg A=m}}\frac{G_k(A)}{A}=\begin{cases}(-1)^m\dfrac{D_m^i}{L_m}, & 若\ k=iq^m\quad(0\leqslant i\leqslant q);\\ 0, & 否则.\end{cases}$$

将上式左端记为 G.

证明 若 $k=iq^m$ $(0\leqslant i\leqslant q)$, 则

$$G=\sum_{\substack{A\in R_1\\ \deg A=m}}\frac{e_m(A)^i}{A}=D_m^i\sum_{\substack{A\in R_1\\ \deg A=m}}A^{-1}=(-1)^m\frac{D_m^i}{L_m}$$

(将(5.4.7)式取对数微商, 令 $z=T^{q^i}$, 得 $\sum_{\substack{A\in R_1\\ \deg A=i}}A^{-1}=(-1)^i/L_i$).

若 $1\leqslant k\leqslant q-1$, 则 $G=0$. 这是由于 $S_m(k-1)=0$, 并且 $G_k(z)$ 是关于 z 的 k 次多项式, 并且 $G_k(0)=0$. 最后若 $k=iq^m+j$ $(1\leqslant i\leqslant q-1, 1\leqslant j<q^m)$, 则 $G_k(z)=e_m(z)^iG_j(z)$. 于是

$$G=D_m^i\sum_{\substack{A\in R_1\\ \deg A=m}}\frac{G_j(A)}{A}=0.$$

这就证明了引理5.4.7. ▌

定理5.4.8 (Lee[46]的定理4.1)设

$$k=q^{k_1}+q^{k_2}+\cdots+q^{k_s}\quad(1\leqslant s\leqslant q-1),$$

则

$$S_m(k-1)=(-1)^m[k_1]_m\cdots[k_s]_m/L_m.$$

证明 由引理5.4.6给出

$$z^k=\sum_{j_1=0}^{k_1}\begin{Bmatrix}k_1\\j_1\end{Bmatrix}e_{j_1}(z)\cdots\sum_{j_s=0}^{k_s}\begin{Bmatrix}k_s\\j_s\end{Bmatrix}e_{j_s}(z),$$

于是

$$S_m(k-1)=\sum_{\substack{A\in K_1\\ \deg A=m}}A^{k-1}=\sum_{j_1=0}^{k_1}\begin{Bmatrix}k_1\\j_1\end{Bmatrix}\cdots\sum_{j_s=0}^{k_s}\begin{Bmatrix}k_s\\j_s\end{Bmatrix}\sum_{\substack{A\in K_1\\ \deg A=m}}\frac{G_h(A)}{A},$$

其中 $h=q^{j_1}+q^{j_2}+\cdots+q^{j_s}$. 由引理5.4.7可知,只有当 $j_1=j_2=\cdots=j_s=m$ 时,最后和式才不为零. 因此

$$\begin{aligned}S_m(k-1)&=\begin{Bmatrix}k_1\\m\end{Bmatrix}\cdots\begin{Bmatrix}k_s\\m\end{Bmatrix}(-1)^m\frac{D_m^s}{L_m}\\&=(-1)^m[k_1]_m\cdots[k_s]_m/L_m.\end{aligned}$$ ∎

现在令

$$P_{i,k}(z)=\sum_{A\in R(i)}(z-A)^k,$$

则 $P_{i,1}(z)=e_i(z)$, $e_i(T^i)=D_i$, $P_{i,k}(T^i)=S_i(k)$.

并且 $e_i(X)-e_i(z)=e_i(X-z)=\prod_{A\in R(i)}(X-(z-A))$.

将上式对 X 作对数微商,得到

$$\begin{aligned}\frac{(-1)^i\begin{bmatrix}i\\0\end{bmatrix}}{e_i(X)-e_i(z)}&=\sum_{A\in R(i)}\frac{1}{X-(z-A)}=\frac{1}{X}\sum_{A\in R(i)}\sum_{k\geqslant 0}(z-A)^kX^{-k}\\&=\frac{1}{X}\sum_{k\geqslant 0}X^{-k}P_{i,k}(z).\end{aligned}$$

令 $U=X^{-1}$, 再由(5.4.7)式得到

$$\sum_{k\geqslant 0}P_{i,k}(z)U^k=\frac{(-1)^i\begin{bmatrix}i\\0\end{bmatrix}U^{q^i-1}}{\sum_{\lambda=0}^{i}(-1)^{i-\lambda}\begin{bmatrix}i\\\lambda\end{bmatrix}U^{q^i-q^\lambda}-e_i(z)U^{q^i}},$$

代入 $z=T^i$, 则有

$$\sum_{k\geqslant 0} S_i(k)U^k = \frac{(-1)^i \begin{bmatrix} i \\ 0 \end{bmatrix} U^{q^i-1}}{\sum\limits_{j=0}^{i} (-1)^{i-j} \begin{bmatrix} i \\ j \end{bmatrix} U^{q^i-q^j} - D_i U^{q^i}}. \quad (5.4.8)$$

定理5.4.9 (Gekeler[18]的定理3.13) 设 $k < q^{i+1}-1$，$k = \sum b_j q^j$ 是 k 的 q-adic 展开. 则

$$S_i(k) = (-1)^r M \prod_{j=0}^{i} L_{i-j}^{q^j(b_j-q+1)} \cdot \Gamma_k,$$

其中 $r = i + \sum\limits_{j=0}^{i-1}(i-j+1)b_j$，$\Gamma_k = \prod\limits_j D_j^{b_j}$ 是 § 4.5中定义的 Гamma 函数，而

$$M = \begin{pmatrix} b_i \\ b_0', b_1', \cdots, b_i' \end{pmatrix} = \frac{(b_i)!}{(b_0')!(b_1')!\cdots(b_i')!},$$

其中

$$b_j' = q - 1 - b_j \quad (0 \leqslant j \leqslant i-1), \quad b_i' = l(k) - i(q-1)$$

(于是 $b_0' + b_1' + \cdots + b_i' = i(q-1) - (b_0 + \cdots + b_{i-1}) + l(k) - i(q-1) = b_i$)，并且若 $b_0', \cdots, b_i'$ 之中有负整数时，规定 $\begin{pmatrix} b_0' + \cdots + b_i' \\ b_0', \cdots, b_i' \end{pmatrix} = 0$.

证明 将(5.4.8)式改写为

$$\sum_{k\geqslant 0} S_i(k)U^k = (-1)^i \frac{D_i}{L_i} U^{q^i-1}$$

$$\times \left(1 + \sum_{j=0}^{i-1} (-1)^{i-j} \begin{bmatrix} i \\ j \end{bmatrix} U^{q^i-q^j} - D_i U^{q^i}\right)^{-1}$$

$$= (-1)^i \frac{D_i}{L_i} U^{q^i-1} \sum_{\lambda\geqslant 0} \left(\sum_{j=0}^{i-1} (-1)^{i-j-1} \begin{bmatrix} i \\ j \end{bmatrix} U^{q^i-q^j}\right.$$

$$\left. + D_i U^{q^i}\right)^\lambda$$

$$= (-1)^i \frac{D_i}{L_i} U^{q^i-1} \sum_{\lambda\geqslant 0} \sum_{\alpha_0,\cdots,\alpha_{i-1},\beta} \begin{pmatrix} \lambda \\ \alpha_0, \cdots, \alpha_{i-1}, \beta \end{pmatrix}$$

$$\times \prod_{j=0}^{i-1}\left((-1)^{(i-j-1)}\begin{bmatrix} i \\ j \end{bmatrix}\right)^{\alpha_j} D_i^{\beta} U^{\sum_{j=0}^{i-1}(q^i-q^j)\alpha_j+\beta q^i},$$

其中关于 $\alpha_0,\cdots,\alpha_{i-1},\beta$ 的求和满足条件：

$$\alpha_0,\cdots,\alpha_{i-1},\ \beta \geqslant 0,\ \alpha_0+\cdots+\alpha_{i-1}+\beta=\lambda.$$

这表明对每个 $k\geqslant 0$，令 $k'=k-(q^i-1)$，则

$$S_i(k)=(-1)^i\frac{D_i}{L_i}$$

$$\times \sum_{\alpha_0,\cdots,\alpha_{i-1},\beta}\begin{Bmatrix}\alpha_0+\cdots+\alpha_{i-1}+\beta \\ \alpha_0,\cdots,\alpha_{i-1},\beta\end{Bmatrix}$$

$$\times \prod_{j=0}^{i-1}\left((-1)^{(i-j-1)}\begin{bmatrix} i \\ j \end{bmatrix}\right)^{\alpha_j} D_i^{\beta}, \tag{5.4.9}$$

其中求和过所有满足

$$\sum_{j=0}^{i-1}\alpha_j(q^i-q^j)+\beta q^i=k' \tag{5.4.10}$$

的 $\alpha_0,\cdots,\alpha_{i-1},\beta$. 当 $k<q^i-1$时，$k'<0$，从而(5.4.10)不存在解 $\alpha_0,\cdots,\alpha_{i-1},\beta\geqslant 0$. 于是 $S_i(k)=0$(或见系5.4.5的(3)). 另一方面，这时 $b_i'=l(k)-i(q-1)<0$，所以 $M=0$. 即定理对于 $k<q^i-1$的情形成立. 以下设 $q^i-1\leqslant k<q^{i+1}-1$. 这时 $k'<q^{i+1}-q^i$，设

$$k'=k-(q^i-1)=a_Nq^N+a_{N+1}q^{N+1}+\cdots+a_iq^i \quad (a_N\geqslant 1) \tag{5.4.11}$$

是 k'的 q-adic 展开. 由于 $k=\sum b_jq^j$ 为 k 的 q-adic 展开，可知当 $N<i$时，

$$\begin{aligned}\sum b_jq^j &= k'+(q^i-1) \\ &= (q-1)+(q-1)q+\cdots \\ &\quad +(q-1)q^{N-1}+(a_N-1)q^N \\ &\quad +a_{N+1}q^{N+1}+\cdots+a_{i-1}q^{i-1}+(a_i+1)q^i.\end{aligned}$$

于是

$$b_j=q-1\quad(0\leqslant j\leqslant N-1),\quad b_N=a_N-1,$$

$$b_j=a_j\quad(N+1\leqslant j\leqslant i-1),$$

$$b_i = a_i + 1.$$

另一方面，由 $k' < q^{i+1} - q^i$，可知满足(5.4.10)的 $\alpha_0, \cdots, \alpha_{i-1}$，$\beta$ 均小于 q. 比较(5.4.10)和(5.4.11)可知有唯一解：

$$\alpha_j = 0 \quad (0 \leqslant j \leqslant N-1), \quad \alpha_N = q - a_N,$$
$$\alpha_j = q - 1 - a_j \quad (N+1 \leqslant j \leqslant i-1),$$
$$\beta = a_i + 1 - \sum_{j=0}^{i-1} \alpha_j.$$

于是 $\alpha_j = q - 1 - b_j = b_j'$ $(0 \leqslant j \leqslant i-1)$，$\beta = b_i'$. 当 $\beta < 0$ 时，$M = 0$，并且(5.4.9)式也给出 $S_i(k) = 0$，所以定理成立. 以下设 $\beta \geqslant 0$. 则(5.4.9)式变成

$$S_i(k) = (-1)^i \frac{D_i}{L_i} M D_i^\beta \prod_{j=0}^{i-1} \left((-1)^{i-j+1} \begin{bmatrix} i \\ j \end{bmatrix} \right)^{\alpha_j}$$
$$= (-1)^{r'} M \frac{D_i^{1+\beta}}{L_i} \prod_{j=0}^{i-1} \left(\frac{D_i}{D_j L_{i-j}^{q^j}} \right)^{q-1-b_j},$$

其中

$$r' = i + \sum_{j=0}^{i-1} (i-j+1)\alpha_j \equiv i + \sum_{j=0}^{i-1} (i-j+1) b_j$$
$$= r \pmod 2.$$

再利用恒等式 $\prod_{j=0}^{s} D_j^{q-1} = D_{s+1}/L_{s+1}$，就得到

$$S_i(k) = (-1)^r M \prod_{j=0}^{i-1} L_{i-j}^{q^j(b_j - q+1)} \cdot D_i^{1+\beta+\alpha_0+\cdots+\alpha_{i-1}-1} \prod_{j=0}^{i-1} D_j^{b_j}$$
$$= (-1)^r M \prod_{j=0}^{i-1} L_{i-j}^{q^j(b_j-q+1)} \cdot \Gamma_k.$$

如果 $N = i$，则 $a_0 = \cdots = a_{i-1} = 0$，$\beta = a_i$. $k = q^i - 1 + \beta q^i$ $(1 \leqslant \beta \leqslant q-1)$，$b_0 = \cdots = b_{i-1} = q-1$，$b_0' = \cdots = b_{i-1}' = 0$. 由(5.4.9)式给出

$$S_i(k) = (-1)^i D_i^{\beta+1} / L_i = (-1)^i \Gamma_k.$$

由于 $r \equiv i \pmod 2$，$M = 1$，可知本定理对于 $N = i$ 的情形也成立. ▌

基于上述结果，现在可以证明以下定理：

定理5.4.10[23],[56] (1) 若 $k=cq^m+(q^m-1)$ $(1\leqslant c<q-1)$，则 $S_m(k)=(-1)^m\Gamma_k$. 而当 $w\geqslant1$时，$S_{m+w}(k)=0$，$\deg S_{m-w}(k)<\deg\Gamma_k$.

(2) 对于 $k=q^m-1$，则 $S_m(k)=(-1)^m\Gamma_k$，$S_{m-1}(k)$的最高次项为$(-1)^{m-1}T^{\deg\Gamma_k}$. 而当 $w\geqslant1$时，$S_{m+w}(k)=0$，$\deg S_{m-1-w}(k)<\deg\Gamma_k$.

(3) 若 $k\neq cq+(q^m-1)$ $(0\leqslant c<q-1)$，则对于每个 $i\geqslant0$，$\deg S_i(k)<\deg\Gamma_k$.

证明 显然有 $\deg S_i(k)\leqslant ik$. 设 $k=\sum_{j=0}^{l}k_jq^j$ 是 k 的 q-adic 展开，我们先证明两个论断：

(A) 若 $S_i(k)\neq0$，$ik\geqslant\deg\Gamma_k$，则当$2\nmid k$ 时 $i=l$，而$2|k$ 时 $i=l$ 或 $l+1$.

现在证明：$\deg\Gamma_k=\sum jk_jq^j$. 再由假设条件$ik\geqslant\deg\Gamma_k$，可知 $i\geqslant l$. 由于 $S_i(k)\neq0$，由定理5.4.4表明 k 可以表示成

$$k=m_0+m_1+\cdots+m_i,\quad q-1|m_j\geqslant1\quad(1\leqslant j\leqslant i),$$

并且上式右端用 p-adic 方式作加法时没有进位，从而用 q-adic 方式作加法也没有进位. 这表明 $l(k)\geqslant i(q-1)+h$，其中 h 是 k 模 $q-1$的最小非负剩余. 但是 $l(k)\leqslant(l+1)(q-1)$，并且当$2\nmid k$ 时，$l(k)\leqslant l(q-1)+h$. 由此即得结论.

(B) 若 $k<q^{l+1}-1$，并且 k 满足定理中的情形(3)，则 $\deg S_l(k)<\deg\Gamma_k$.

证明由定理5.4.9推出. 因为此时存在 $j\geqslant1$，使得 $k_j\neq q-1$.

现在设 $k=cq^m+(q^m-1)$，$0\leqslant c<q-1$. 由定理5.4.8可知当 $c=0$时，$S_m(k)=(-1)^m\Gamma_k$. 而当$1\leqslant c<q-1$时，

$$S_m(k)=(-1)^mD'_m(D_0\cdots D_{m-1})^{q-1}=(-1)^m\Gamma_k.$$

本定理的其他论断可由(A)和(B)推出. ▌

由于 $\beta_k(T)$和 $S_i(k)$有本节开头所述的关系，并且对于§4.1定义的 Goss zeta 函数 $\zeta_\infty(s)$有 $\zeta_\infty(-k)=\beta_k(T)$ (当$(q-1)\nmid k$ 时)；$\zeta_\infty(-k)=0$ (当$(q-1)|k$ 时)，所以定理5.4.10直接给出了

如下推论：

系5.4.11　对于定理5.4.10的三种情形，分别有：

(1) $\zeta_\infty(-k)$和$\beta_k(T)$的最高次项均为$(-1)^m T^{\deg\Gamma_k}$.

(2) $\beta_k(T)$的最高次项为$(-1)^{m-1}T^{\deg\Gamma_k}$，而$\zeta_\infty(-k)=0$.

(3) $\deg\zeta_\infty(-k)<\deg\Gamma_k$，$\deg\beta_k(T)<\deg\Gamma_k$.　▌

系5.4.12　设$k=\sum k_j q^j$为k的q-adic展开，$\Gamma_k=\prod_j e_j(z)^{k_j}=\sum_{i=0}^{k}a_i z^i$，则对每个$i\geqslant 0$，有

$$\deg a_i+\deg\zeta_\infty(-i)\leqslant\deg\Gamma_k.$$

上式的等式成立当且仅当$k=cq^m+(q^m-1)$ $(1\leqslant c<q-1)$，同时$i=k$.

证明　当$i=k$时，$a_k=1$，定理可由系5.4.11推出. 对于一般的u $(0\leqslant u\leqslant k)$，如果$a_u\neq 0$，则必然有

$$u=q^{u_1}+\cdots+q^{u_b},b=\sum_j k_j.$$

又设$a_v\neq 0$，$v=q^{c_1}+\cdots+q^{c_b}$，其中$a_j=c_j$ $(1\leqslant j\leqslant b-1)$，而$a_b=c-d$，$c_b=c$ $(d>0)$. 这时$v=u+q^c-q^{c-d}>u$. 由于

$$\deg\binom{j}{c-d}-\deg\binom{j}{c}=\deg\binom{c}{c-d},$$

$$\deg\Gamma_{v+q^c}-\deg\Gamma_{v+q^{c-d}}\geqslant\deg\binom{c}{c-d},$$

可知$\deg a_u+\deg\Gamma_u\leqslant\deg a_v+\deg\Gamma_v$. 于是归纳可证得：

$$\deg a_u+\deg\zeta_\infty(-u)\leqslant\deg a_u+\deg\Gamma_u$$

$$\leqslant\deg a_v+\deg\Gamma_v\leqslant\deg\Gamma_k$$

(最后一个不等式用了归纳假设). 再注意到当$k\neq cq^m+(q^m-1)$ $(1\leqslant c<q-1)$时，$\deg\zeta_\infty(-u)<\deg\Gamma_u$，即给出了等式成立的条件.　▌

注记　定理5.4.10和系5.4.11最早是由Goss[23],[25]通过大量计算数据提出的猜想. 后来由Gekeler[18]所证明，并且又发现这在很早之前已经由Lee[46]所证明了，我们在这里混合采用了Lee和

Gekeler 的方法.

§5.5 分布与测度

现在介绍局部环 R_P 上的积分理论. 由 B. Mazur 和 N. Katz 等人系统发展的分布和测度理论是分圆域理论等现代数论的有用工具. 这一工具由 Galovich 和 Rosen[37]以及 Goss[29]等人利用到分圆函数域. 如前一样，令 $k=\boldsymbol{F}_q(T)$，$R=\boldsymbol{F}_q[T]$，P 是 R 中 d 次首1不可约多项式，k_P 为 k 对有限素除子 P 的局部化，R_P 是 R 对于素理想 P 的局部化. 即

$$R_P=\{\alpha\in k_P:|\alpha|_P\leqslant 1\}=\{\alpha\in k_P:v_P(\alpha)\geqslant 0\},$$

其中 $|\alpha|_P$ 和 v_P 分别为 k 关于 P 的标准赋值和标准指数赋值.

和数域的情形一样，R_P 上的积分可以有三种不同观点：射影系 $R_P=\varprojlim R/(P^n)$ 上的分布(和测度)；定义在 R_P 的紧开子集族上的可加性映射；以及 R_P 上连续函数空间上的(有界)泛函. 关于 p-adic 整数环 $\boldsymbol{Z}_p=\varprojlim \boldsymbol{Z}/(p^n)$ 上积分的这三种观点参看 Koblitz、Washington 或 S. Lang 的书[42],[57],[45]. 现在对于 R_P 上的积分依次介绍这三种观点：

对于 $i\geqslant j\geqslant 1$，有环的自然满同态：

$$\pi_{ij}:R/(P^i)\to R/(P^j),\quad A\pmod{P^i}\mapsto A\pmod{P^j},$$

则 $\{R/(P^n),\ \pi_{ij}\mid n\geqslant 1, i\geqslant j\geqslant 1\}$ 形成射影系，即 π_{ii} 是恒等映射，并且当 $i\geqslant j\geqslant k$ 时，$\pi_{jk}\pi_{ij}=\pi_{ik}$. 这个射影系的射影极限：

$$\varprojlim R/(P^n)=\{(\alpha_1,\alpha_2,\cdots,\alpha_n,\cdots)\mid \alpha_n\in R/(P^n),\pi_{ij}(\alpha_i)=\alpha_j$$

(当 $i\geqslant j$ 时)$\}$ 自然等同于局部环 R_P，即 R_P 中的元素：

$$\alpha=A_0+A_1P+A_2P^2+\cdots+A_nP^n+\cdots\quad (A_i\in R,\ \deg A_i<d)$$

自然等同于 $\varprojlim R/(P^n)$ 中的元素 $(\alpha_1,\alpha_2,\cdots,\alpha_n,\cdots)$，其中

$$\alpha_n=\sum_{i=0}^{n-1}A_iP^i\pmod{P^n}=\alpha\pmod{P^n}.$$

对于每个 $n\geqslant 1$，有环的满同态：

$$\pi_n: R_P \to R/(P^n), \quad \alpha \mapsto \alpha_n.$$

$\mathrm{Ker}(\pi_n)$ 为 R_P 的理想 $(P^n)=P^nR_P$. 从而 $R/(P^n)$ 中的每个元素的原象为 $A+(P^n)$，其中不妨设 $A\in R$，$\deg A<nd$. R_P 中每个这样的集合 $A+(P^n)$ $(A\in R, n\geqslant 1)$ 称作 R_P 的区间，它是 R_P 的紧开子集，并且所有的区间形成拓扑环 R_P 的一个基本邻域系.

定义5.5.1　设 G 为阿贝尔群. 映射族

$$\{\varphi_n: R/(P^n) \to G\} \quad (n=1,2,3,\cdots)$$

称作射影系 $\{R/(P^n),\pi_{ij}\}$ 的一个取值于 G 的分布，是指对每个 $x\in R/(P^j)$ 和 $i\geqslant j$，均有

$$\varphi_j(x) = \sum_{\substack{y\in R/(P^i)\\ \pi_{ij}(y)=x}} \varphi_i(y). \tag{5.5.1}$$

由于该射影系的下标集合 $\{1,2,3,\cdots,n,\cdots\}$ 是线性序列，所以只需对 $i=j+1$ 的情形(5.5.1)式成立即可，即分布所满足的条件为：对每个 $j\geqslant 1$ 和 $x\in R/(P^j)$，有

$$\varphi_j(x) = \sum_{\substack{y\in R/(P^{j+1})\\ y\equiv x \pmod{P^j}}} \varphi_{j+1}(y) = \sum_{\substack{B\in R\\ \deg B<d}} \varphi_{j+1}(x+BP^j). \tag{5.5.2}$$

通过映射族 $\{\pi_n\}$ $(n\geqslant 1)$ 可以把(5.5.2)式提升到 R_P 上. 对每个 $x\in R/(P^n)$，我们定义 $\varphi(x+(P^n))=\varphi_n(x)$，这就给出一个映射 φ，它把 R_P 的每个区间映成 G 中的元素，而(5.5.2)式转变成下面的(5.5.3)式，所以定义5.5.1就转变成定义5.5.1′：

定义5.5.1′　设 G 为阿贝尔群. 在 R_P 上取值于 G 的分布是一个映射 φ，它把 R_P 的每个区间映成 G 中的元素，并且对每个 $A\in R$ 和 $n\geqslant 1$，有

$$\varphi(A+(P^n)) = \sum_{\substack{B\in R\\ \deg B<d}} \varphi(A+BP^n+(P^{n+1})). \tag{5.5.3}$$

与拓扑环 $\mathbf{Z}_p$ 的情形一样，环 R_P 的每个紧开子集都是有限个两两非交的区间的并(证明可参见 Koblitz[42]). 设 φ 是 R_P 上取值

于 G 的分布，如果 R_p 的紧开子集 B 是两两非交的区间 $B_1,\cdots,B_t$ 的并，我们令

$$\varphi(B)=\varphi(B_1)+\cdots+\varphi(B_t),$$

利用(5.5.3)式可以证明，$\varphi(B)$ 和上述 $B_1,\cdots,B_t$ 的取法无关. 这就把映射 φ 的定义域扩充到了 R_p 的所有紧开子集上，并且 φ 满足可加性，即若紧开子集 B 是两两非交的有限个紧开子集 $B_1,\cdots,B_t$ 的并，则 $\varphi(B)=\varphi(B_1)+\cdots+\varphi(B_t)$. 所以我们给出 R_p 上分布的第二个定义如下：

定义5.5.2 设 G 是阿贝尔群. R_p 上取值于 G 的一个分布是指可加性映射

$$\varphi:\{R_p\text{ 的紧开子集}\}\to G.$$

以下我们取 G 为 C_p(k_p 的代数闭包的拓扑完备化域). 令 $\mathscr{P}$ 是 P 到域 C_p 的唯一扩充素除子，$|\ \ |_{\mathscr{P}}$ 是 k 中赋值 $|\ \ |_P$ 到 C_p 的唯一扩充. 我们用 $C(R_p)$ 表示从 R_p 到 C_p 的所有连续函数组成的 C_p 上的向量空间. 对每个 $f\in C(R_p)$，定义 f 的范数为

$$\|f\|=\operatorname*{Max}_{a\in R_p}|f(a)|_{\mathscr{P}},$$

则 $C(R_p)$ 对这个范数是 Banach 空间(完备赋范空间).

设 φ 是 R_p 上取值于 C_p 的分布，对于 R_p 的每个紧开子集 B，令 χ_B 是 B 的特征函数，即

$$\chi_B(x)=\begin{cases}1, & \text{若 } x\in B;\\ 0, & \text{否则}.\end{cases}$$

我们把 $\varphi(B)$ 写成如下形式：

$$\varphi(B)=\int_{R_p}\chi_B(x)d\varphi(x)=\int_B d\varphi(x),$$

称作函数 χ_B(对于分布 φ)的积分. 函数 $f\in C(R_p)$ 称作是局部常值的，是指对每个 $x\in R_p$ 均有包含 x 的紧开子集 B，使得 f 在 B 上取常值. 熟知全体局部常值函数构成的集合 $S(R_p)$ 是 $C(R_p)$ 的子空间. 对每个局部常值函数 f，R_p 都可以分解成有限个两两非交的紧开子集 $B_1,\cdots,B_t$ 的并，使得 f 在每个 B_i 上取常值 $c_i\in C_p$. 于

是 f 是有限个 χ_{B_i} 的 C_P-线性组合：$f=\sum_{i=1}^{t}c_i\chi_{B_i}$. 我们定义 f 对于分布 φ 的积分为

$$\int_{R_P}f(x)d\varphi(x)=\sum_{i=1}^{t}c_i\int_{R_P}\chi_{B_i}(x)d\varphi(x)$$

$$=\sum_{i=1}^{t}c_i\int_{B_i}d\varphi(x)=\sum_{i=1}^{t}c_i\varphi(B_i).$$

于是 φ 就成为 C_P-向量空间 $S(R_P)$ 上的 C_P-线性泛函：

$$\varphi: S(R_P)\to C_P,\quad f\mapsto\int_{R_P}f(x)d\varphi(x),$$

这就是 R_P 上取值于 C_P 的分布的第三种定义方式.

定义5.5.3　R_P 上取值于 C_P 的分布 φ 称作是测度，是指存在常数 $N>0$，使得对 R_P 的每个紧开子集 B，均有 $|\varphi(B)|_{\mathscr{P}}=\left|\int_B d\varphi(x)\right|_{\mathscr{P}}\leqslant N$.

由于赋值的非阿性质以及每个紧开子集都是有限个两两非交的区间的并，可知定义5.5.3中只要对 R_P 的每个区间 B 满足所述的有界条件即可. 同样由于赋值的非阿性质，可知若 φ 是 R_P 上取值于 C_P 的测度，则对每个局部常值函数 $f\in S(R_P)$，也有 $\left|\int_{R_P}f(x)d\varphi(x)\right|_{\mathscr{P}}\leqslant N$. 又熟知 $S(R_P)$ 是 $C(R_P)$ 的稠密子空间，即对每个连续函数 $f\in C(R_P)$ 均存在局部常值函数序列 $f_n\in S(R_P)$ $(n=1,2,\cdots)$，使得

$$\varepsilon_n=\|f-f_n\|\to 0\ \ (\text{当 } n\to\infty \text{ 时}).$$

这时若 φ 是测度，则

$$\left|\int_{R_P}f_n(x)d\varphi(x)-\int_{R_P}f_m(x)d\varphi(x)\right|_{\mathscr{P}}$$

$$=\left|\int_{R_P}(f_n(x)-f_m(x))d\varphi(x)\right|_{\mathscr{P}}$$

$$\leqslant\|f_n-f_m\|\varphi(R_P)$$

$$\leqslant (\|f_n - f\| + \|f_m - f\|)N \to 0 \ (\text{当 } n,m \to \infty \text{ 时}).$$

这就表明极限$\lim\limits_{n\to\infty}\int_{R_P} f_n(x)d\varphi(x)$存在.我们将这个极限定义成连续函数$f$对于$\varphi$的积分$\int_{R_P} f(x)d\varphi(x)$.于是,下面三个概念是等价的:

(1) φ为R_P上取值于C_P的测度;

(2) φ为有界的可加性映射$\varphi:\{R_P$的紧开子集$\}\to C_P$;

(3) φ为有界C_P-线性泛函$\varphi: C(R_P)\to C_P, f\mapsto \int_{R_P} f(x)d\varphi(x)$

$\Big($这里所指的有界性是指存在$N>0$,使得对每个$f\in C(R_P)$,有

$\left|\int_{R_P} f(x)d\varphi(x)\right|_{\wp} \leqslant \|f\|N\Big)$.

举例如下:

例1 (Dirac 测度) 对于$a\in R_P$,定义映射

$$\delta_a: \{R_P \text{ 的紧开子集}\} \to C_P,$$

其中对R_P的每个紧开子集B,有

$$\delta_a(B) = \begin{cases} 1, & \text{若 } a \in B; \\ 0, & \text{否则}. \end{cases}$$

易知δ_a是R_P上的测度,称作对于a的 Dirac 测度.对于每个连续函数$f\in C(R_P)$,有

$$\int_{R_P} f(x)d\delta_a(x) = f(a).$$

例2 (Beta 测度和 zeta 测度) 设P是$F_q[T]=R$中d次首1不可约多项式($d\geqslant 1$),对R_P的每个区间$A+(P^m)$(其中$m\geqslant 0$, $A\in R$, $\deg A<md$),定义

$$\mu(A+(P^m)) = \begin{cases} 2, & \text{若 } A \in R_1; \\ 1, & \text{否则}. \end{cases}$$

$$\bar{\mu}(A+(P^m)) = \begin{cases} 2+\deg A - md, & \text{若 } A \in R_1; \\ 1+\deg A - md, & \text{若 } A \in R - R_1, A \neq 0; \\ 0, & \text{若 } A = 0. \end{cases}$$

定理5.5.4 μ 和 $\bar{\mu}$ 是 R_P 上取值于 $\boldsymbol{F}_q(\subseteq C_P)$ 的测度. 并且对每个 $k\geqslant 0$，有

$$\int_{R_p} x^k d\mu(x) = \zeta_\infty(-k),\quad \int_{R_p} x^k d\bar{\mu}(x) = \beta_k(T)$$

（μ 和 $\bar{\mu}$ 分别称为 zeta 测度和 beta 测度）.

证明 设 $m\geqslant 0$，$A\in R$，$\deg A< md$. 则

$$\begin{aligned}
&\sum_{\substack{B\in R\\ \deg B<d}} \mu(A+BP^m+(P^{m+1}))\\
&\qquad = \mu(A+(P^{m+1})) + 2\sum_{\substack{B\in R_1\\ \deg B<d}} 1 + \sum_{\substack{B\in R-R_1\\ \deg B<d\\ B\neq 0}} 1\\
&\qquad = \mu(A+(P^m)) + \sum_{\substack{B\in R_1\\ \deg B<d}} 1 + \sum_{\substack{B\in R\\ \deg B<d\\ B\neq 0}} 1\\
&\qquad = \mu(A+(P^m)) + \sum_{\substack{B\in R_1\\ \deg B<d}} 1 + \sum_{\substack{B\in R_1\\ \deg B<d}} \sum_{a\in F_q^*} 1\\
&\qquad = \mu(A+(P^m)) + q\sum_{\substack{B\in R_1\\ \deg B<d}} 1\\
&\qquad = \mu(A+(P^m)).
\end{aligned}$$

所以 μ 是测度. 类似地

$$\begin{aligned}
&\bar{\mu}(A+BP^m+(P^{m+1}))\\
&\quad = \bar{\mu}(A+(P^{m+1})) + \sum_{\substack{B\in R_1\\ \deg B<d}} 1\\
&\qquad + \sum_{\substack{B\in R\\ \deg B<d\\ B\neq 0}} (1+\deg(BP^m)-(m+1)d)\\
&\quad = \bar{\mu}(A+(P^m)) - d + \sum_{\substack{B\in R\\ \deg B<d\\ B\neq 0}} (\deg B - d)\\
&\quad = \bar{\mu}(A+(P^m)) + \sum_{\substack{B\in R\\ \deg B<d\\ B\neq 0}} \deg B
\end{aligned}$$

$$= \overline{\mu}(A + (P^n)) + (q-1) \sum_{\substack{B \in R_1 \\ \deg B < d}} \deg B$$

$$= \overline{\mu}(A + (P^n)) - \sum_{i=1}^{d-1} iq^i = \overline{\mu}(A + (P^n)).$$

所以 $\overline{\mu}$ 也是测度.

现在证明$\int_{R_p} x^k d\mu(x) = \zeta_\infty(-k)$. 当 $k=0$时,两端均为1. 以下设 $k \geqslant 1$. 对每个 $n \geqslant 1$,如果 x、$y \in R_P$, $x \equiv y \pmod{P^n}$,则 $x^k \equiv y^k \pmod{P^n}$. 因此

$$\int_{R_p} x^k d\mu(x) = \sum_{\substack{A \in R \\ \deg A < nd}} \int_{A+(P^n)} x^k d\mu(x)$$

$$\equiv \sum_{\substack{A \in R \\ \deg A < nd}} A^k \mu(A + (P^n)) \pmod{P^n}$$

$$= \sum_{\substack{A \in R \\ \deg A < nd}} A^k + \sum_{\substack{A \in R_1 \\ \deg A < nd}} A^k. \qquad (5.5.4)$$

如果$(q-1) | k$,则(5.5.4)式右端为

$$\sum_{\substack{A \in R_1 \\ \deg A < nd}} \sum_{a \in F_q^*} (aA)^k + \sum_{\substack{A \in R_1 \\ \deg A < nd}} A^k$$

$$= (q - 1 + 1) \sum_{\substack{A \in R_1 \\ \deg A < nd}} A^k = 0.$$

这表明$\int_{R_p} x^k d\mu(x) \equiv 0 \pmod{P^n}$. 令 $n \to +\infty$,可知$\int_{R_p} x^k d\mu(x) = 0 = \zeta_\infty(-k)$. 如果$(q-1) \nmid k$,则(5.5.4)式右端的第一个和式为零. 因此

$$\int_{R_p} x^k d\mu(x) \equiv \sum_{\substack{A \in R_1 \\ \deg A < nd}} A^k \pmod{P^n}.$$

令 $n \to \infty$,可知 $\int_{R_p} x^k d\mu(x) = \sum_{A \in R_1} A^k = \zeta_\infty(-k)$. 最后证明 $\int_{R_p} x^k d\overline{\mu}(x) = \beta_k(T)$. 当 $k=0$时,两边均为0. 以下设 $k \geqslant 1$. 这时有

$$\int_{R_P} x^k d\overline{\mu}(x) \equiv \sum_{\substack{A\in R\\ \deg A<nd}} A^k \overline{\mu}(A+(P^n)) \pmod{P^n}$$
$$= \sum_{\substack{A\in R\\ \deg A<nd\\ A\neq 0}} A^k(1+\deg A-nd) + \sum_{\substack{A\in R_1\\ \deg A<nd}} A^k. \tag{5.5.5}$$

如果$(q-1)|k$,则(5.5.5)式右端为

$$-\sum_{\substack{A\in R_1\\ \deg A<nd}} A^k(\deg A-nd) = -\sum_{\substack{A\in R_1\\ \deg A<nd}} A^k\deg A - nd\sum_{\substack{A\in R\\ \deg A<nd\\ A\neq 0}} A^k.$$

取一个固定多项式B使得$(B,P)=1$，$\deg B\geqslant 1$,这时有

$$\sum_{\substack{0\neq A\in R\\ \deg A<nd}} A^k \equiv \sum_{A\in R/(P^n)} A^k \pmod{P^n}$$
$$\equiv \sum_{A\in R/(P^n)} (AB)^k = B^k \sum_{A\in R/(P^n)} A^k \pmod{P^n}.$$

这就表明

$$(B^k-1)\sum_{\substack{0\neq A\in R\\ \deg A<nd}} A^k \equiv 0 \pmod{P^n}.$$

于是

$$v_P\Big(\sum_{\substack{0\neq A\in R\\ \deg A<nd}} A^k\Big) \geqslant n - v_P(B^k-1) \geqslant n - \left[\frac{k\deg B}{d}\right].$$

当$n\to+\infty$时,上式右端趋于$+\infty$. 这就表明

$$\int_{R_P} x^k d\overline{\mu}(x) = -\sum_{A\in R_1} A^k \deg A = \beta_k(T).$$

如果$(q-1)\nmid k$,则(5.5.5)式右端第一个和式为零. 于是

$$\int_{R_P} x^k d\overline{\mu}(x) = \sum_{A\in R_1} A^k = \beta_k(T).$$

这就证明了定理5.5.4. ▌

以$\mathscr{M}$表示R_P上取值于C_P的所有测度组成的集合. 对于$\mu,\nu\in\mathscr{M}$,自然定义加法运算和卷积运算$\mu*\nu$为:对每个$f\in C(R_P)$,有

$$\int_{R_p} f(x)d(\mu+\nu)(x)=\int_{R_p} f(x)d\mu(x)+\int_{R_p} f(x)d\nu(x),$$

$$\int_{R_p} f(x)d(\mu*\nu)(x)=\int_{R_p}\int_{R_p} f(x+y)d\mu(x)d\nu(y).$$

由定义知 $\mu*\nu=\nu*\mu$，并且 $\mathscr{M}$ 对于这两种运算形成域 C_P 上的交换代数$\left(\text{对于 } a\in C_P, \int f(x)d(a\mu)(x)=a\int f(x)d\mu(x)\right)$. 利用§5.1的结果，可以把这个交换代数表示成另一种形式. 根据定理5.1.5，$C(R_P)$中每个连续函数 $f(x)$ 均唯一地表示成

$$f(x)=\sum_{j\geqslant 0} a_j\frac{G_j(x)}{\Gamma_j}, \tag{5.5.6}$$

其中 $a_j\in C_p$，$a_j\to 0$（对于 P-adic 拓扑）. 对于 $\mu\in\mathscr{M}$，令

$$b_j=\int_{R_p}\frac{G_j(x)}{\Gamma_j}d\mu(x)\quad(j=0,1,2,\cdots),$$

则 $b_j\in C_P$. 由于 $G_j(x)/\Gamma_j$ 是从 R_P 到 R_P 的连续函数（见定理5.1.5前面所述），可知 $b_j(j=0,1,2,\cdots)$是有界的，即存在 $N>0$，使得 $|b_j|_{\mathscr{P}}\leqslant N$ $(j=0,1,2,\cdots)$. 于是对于由(5.5.6)式表出的 $f(x)\in C(R_P)$，有

$$\int_{R_p} f(x)d\mu(x)=\sum_{j\geqslant 0} a_j\int_{R_p}\frac{G_j(x)}{\Gamma_j}d\mu(x)=\sum_{j\geqslant 0} a_jb_j\in C_P.$$

如果又有 $\nu\in\mathscr{M}$，并且

$$c_j=\int_{R_p}\frac{G_j(x)}{\Gamma_j}d\nu(x)\quad(j=0,1,2,\cdots),$$

则

$$\begin{aligned}\int_{R_p}\frac{G_j(x)}{\Gamma_j}d(\mu*\nu)(x)&=\int_{R_p}\int_{R_p}\frac{G_j(x+y)}{\Gamma_j}d\mu(x)d\nu(y)\\&=\int_{R_p}\int_{R_p}\sum_{\substack{e+f=j\\e,f\geqslant 0}}\binom{j}{e}\frac{G_e(x)}{\Gamma_e}\cdot\frac{G_f(y)}{\Gamma_f}d\mu(x)d\nu(y)\end{aligned}$$

（加法公式，可类似于引理 5.1.4(1) 证明）

$$=\sum_{e+f=j}\binom{j}{e}\int_{R_p}\frac{G_e(x)}{\Gamma_e}d\mu(x)\int_{R_p}\frac{G_f(y)}{\Gamma_f}d\nu(y)$$

$$= \sum_{e+f=j} \binom{j}{e} b_e c_f = \sum_{e=0}^{j} \binom{j}{e} b_e c_{j-e}. \qquad (5.5.7)$$

现在我们考虑集合

$$\mathscr{D} = \left\{ \sum_{j=0}^{\infty} b_j \frac{Z^j}{j!} \middle| b_j \in C_P, \text{并且存在 } N > 0, \text{使得 } |b_j| \leqslant N \right.$$
$$\left. (j = 0,1,2,\cdots) \right\}$$

这里对每个 $j \geqslant 0$，$\frac{Z^j}{j!}$ 看成一个符号. 于是有映射

$$\varphi: \mathscr{M} \to \mathscr{D}, \quad \mu \mapsto \sum_{j \geqslant 0} b_j \frac{Z^j}{j!},$$

其中 $b_j = \int_{R_P} \frac{G_j(x)}{\Gamma_j} d\mu(x)$. 这显然是 C_P-线性映射. 由定理5.1.5可知这是一一对应，即 φ 是 C_P-向量空间的同构. 进而在 $\mathscr{D}$ 中自然引入加法和乘法：

$$\sum a_j \frac{Z^j}{j!} + \sum b_j \frac{Z^j}{j!} = \sum (a_j + b_j) \frac{Z^j}{j!},$$

$$\left(\sum_{j \geqslant 0} a_j \frac{Z^j}{j!} \right) \cdot \left(\sum_{k \geqslant 0} b_k \frac{Z^k}{k!} \right) = \sum_{j,k \geqslant 0} a_j b_k \left(\frac{Z^j}{j!} \cdot \frac{Z^k}{k!} \right)$$
$$= \sum_{j,k \geqslant 0} a_j b_k \frac{(j+k)!}{j!k!} \cdot \frac{Z^{j+k}}{(j+k)!} = \sum_{i \geqslant 0} c_i \frac{Z^i}{i!},$$

其中

$$c_i = \sum_{\substack{j+k=i \\ j,k \geqslant 0}} a_j b_k \frac{i!}{j!k!} = \sum_{j=0}^{i} \binom{i}{j} a_j b_{i-j}.$$

则 $\mathscr{D}$ 由此成为 C_P-交换代数. 由(5.5.7)式可知有以下结论：

定理5.5.5 (Goss[29]) 上述映射 φ 是 $\mathscr{M}$ 到 $\mathscr{D}$ 的 C_P 上的交换代数同构. ▌

对于 $\mu \in \mathscr{M}$,

$$\varphi(\mu) = \sum_{j \geqslant 0} b_j \frac{Z^j}{j!} \quad \left(\text{其中 } b_j = \int_{R_P} \frac{G_j(x)}{\Gamma_j} d\mu(x) \right)$$

称作测度 μ 的 divided 幂级数.

例1 对于前述的 Dirac 测度 δ_a $(a\in R_P)$，则有

$$b_j=\int_{R_P}\frac{G_j(x)}{\Gamma_j}d\delta_a(x)=\frac{G_j(a)}{\Gamma_j}\quad(j\geqslant 0).$$

于是 $\varphi(\delta_a)=\sum_{j\geqslant 0}\frac{G_j(a)}{\Gamma_j}\cdot\frac{Z^j}{j!}$. 特别是 $\varphi(\delta_0)=1$，所以 δ_0是代数 $\mathscr{M}$ 中的幺元素.

例2 现在求定理5.5.4给出的 zeta 测度 μ 和 beta 测度 $\bar{\mu}$ 的幂级数. 这是由 D. Goss 通过计算提出的猜想而由 Thakur[56]证明的.

定理5.5.6 (1) 设 zeta 测度 μ 的幂级数为$\sum_{k\geqslant 0}\mu_k\frac{Z^k}{k!}$,则

$$\mu_k=\begin{cases}(-1)^m, & 若\ k=cq^m+(q^m-1)\quad(0<c<q-1);\\ 0, & 否则.\end{cases}$$

(2) 设 beta 测度 $\bar{\mu}$ 的幂级数为$\sum_{k\geqslant 0}\bar{\mu}_k\frac{Z^k}{k!}$,则

$$\bar{\mu}_k=\begin{cases}(-1)^m, 若\ k=cq^m+(q^m-1)\quad(0<c\leqslant q-1);\\ 0, 否则.\end{cases}$$

证明 (1) 首先,由于 $\mu_k=\int_{R_P}\frac{G_k(x)}{\Gamma_k}d\mu(x)$, $\frac{G_k(x)}{\Gamma_k}\in\boldsymbol{F}_q(T)[x]$, 而$\int_{R_P}x^i d\mu(x)=\zeta(-i)\in R=\boldsymbol{F}_q[T]$, 可知 $\mu_k\in\boldsymbol{F}_q(T)$. 进而,对每个首1不可约多项式 P,当 $x\in R_P$ 时,$\frac{G_k(x)}{\Gamma_k}\in R_P$. 再由测度 μ 取值于 $R\subseteq R_P$,所以 $\mu_k\in R_P$(对每个 P). 这就证明了 $\mu_k\in R=\boldsymbol{F}_q[T]$.

现在设 $G_k(x)=\sum_{i=0}^{k}a_ix^i$ $(a_i\in R)$. 则

$$\mu_k=\int_{R_P}\frac{G_k(x)}{\Gamma_k}d\mu(x)=\sum_{i=0}^{k}\frac{a_i\zeta_\infty(-i)}{\Gamma_k}\in R.$$

根据上节的系5.4.12，当 $k\neq cq^m+(q^m-1)$ $(1\leqslant c<q-1)$时，

$$\deg\left(\frac{a_i\zeta_\infty(-i)}{\Gamma_k}\right)<0\quad(0\leqslant i\leqslant k).$$

这表明了
$$\mu_k = \sum_{i=0}^{k} \frac{a_i \zeta_\infty(-i)}{\Gamma_k} = 0.$$

当 $k=cq^m+(q^m-1)$ $(1\leqslant c<q-1)$时，由系5.4.12可知

$$\deg\left(\frac{a_i \zeta_\infty(-i)}{\Gamma_k}\right) < 0 \quad (0 \leqslant i \leqslant k-1), \quad \deg\left(\frac{a_k \zeta_\infty(-k)}{\Gamma_k}\right) = 0.$$

所以 μ_k 等于$\frac{a_k \zeta_\infty(-k)}{\Gamma_k}$的常数项. 但是 $a_k=1$，而 $\zeta_\infty(-k)$的最高次项为$(-1)^m T^{\deg \Gamma_k}$(由系5.4.11)，这就表明 $\mu_k=(-1)^m$.

(2) 利用系5.4.12和5.4.11，可类似地证明. ▌

分布和测度理论以及 p-adic 分析工具在研究数域的分圆域理论中起着重要的作用. 人们也期望本章所介绍的分析理论在研究分圆函数域时会起到更大的作用(见文献[30]和[31]).

附　　录

§6.1 高次互反律

设 P 为 $R=\boldsymbol{F}_q[T]$中首 1 不可约多项式，其中 $2\nmid q$. 记$|P|=q^{\deg P}$，则$(R/(P)^*)$是$|P|-1$ 阶循环群. 对每个多项式 $A\in R$，$P\nmid A$，存在唯一的元素$\left\{\frac{A}{P}\right\}\in\boldsymbol{F}_q^*$，使得

$$\left\{\frac{A}{P}\right\}\equiv A^{\frac{|P|-1}{q-1}}\pmod P.$$

于是：$\left\{\frac{A}{P}\right\}=1$当且仅当存在 $B\in R$，使得 $A\equiv B^{q-1}\pmod P$(即 A 是模 P 的 $q-1$次剩余). 更一般地，对 $q-1$的每个正因子 m，有 $q-1=me$. 则$\left\{\frac{A}{P}\right\}^e=1$当且仅当 A 是模 P 的 m 次剩余. 由定义不难看出：

(1) 若 $a\in\boldsymbol{F}_q^*$，则$\left\{\frac{a}{P}\right\}=a^{\frac{|P|-1}{q-1}}$；

(2) 若 A、$B\in R$，$P\nmid AB$，则$\left\{\frac{AB}{P}\right\}=\left\{\frac{A}{P}\right\}\cdot\left\{\frac{B}{P}\right\}$；

(3) 若 A、$B\in R$，$A\equiv B\not\equiv 0\pmod P$，则$\left\{\frac{A}{P}\right\}=\left\{\frac{B}{P}\right\}$.

所以，为了计算$\left\{\frac{A}{P}\right\}$，我们只需考虑 A 是首1不可约多项式的情形即可. 对于这种情形，有如下定理：

定理　($\boldsymbol{F}_q[T]$上的高次互反律)　设 P 和 Q 是 $R=\boldsymbol{F}_q[T]$中

不同的首1不可约多项式. 则

$$\left\{\frac{P}{Q}\right\}\cdot\left\{\frac{Q}{P}\right\}^{-1}=(-1)^{\deg P\cdot\deg Q}=(-1)^{\frac{|P|-1}{q-1}\cdot\frac{|Q|-1}{q-1}}$$

$\left(最后的等式是由于\frac{|P|-1}{q-1}=\frac{q^{\deg P}-1}{q-1}\equiv\deg P\pmod 2\right)$.

就作者所知,这个定理最早是由 Kuhne 于1901年证明的. 就像 $\mathbf{Z}$ 上的高斯二次互反律的情形一样, 后来又发现了不少新的证明(如 F. K. Schmidt、Carlitz、Hellegouarch 等等). 在上述工作中, 高次互反律的证明大都包含在关于 $\mathbf{F}_q[T]$的一些更一般的性质或计算之中. 在本附录中,我们提供高次互反律的五个证明. 其中第一个证明是初等的,另四个证明则使用 Carlitz 模和分圆函数域理论.

第一个证明 是高斯对古典二次互反律

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

给出的一个证明的模拟. 对 $R=\mathbf{F}_q[T]$中每个非零多项式 A,以 $\mathrm{sgn}(A)$表示 A 的首项系数,而$[A]_P$ 表示 A 被 P 除得到的剩余多项式. 又记

$$\mathscr{M}=\mathscr{M}(P)=\{A\in R:0\leqslant\deg A<\deg P\},$$

$$\mathscr{M}_1=\mathscr{M}_1(P)=\{A\in\mathscr{M}(P):\mathrm{sgn}(A)=1\}.$$

下面的引理是关于 Legendre 符号的高斯引理的模拟.

引理6.1.1 设 P 为 $\mathbf{F}_q[T]$中首1不可约多项式,$A\in\mathbf{F}_q[T]$, $P\nmid A$,则

$$\left\{\frac{A}{P}\right\}=\prod_{B\in\mathscr{M}_1(P)}\mathrm{sgn}([AB]_P).$$

证明 对每个 $a\in\mathbf{F}_q^*$, $[aA]_P=a[A]_P$. 所以当 B 过 $\mathscr{M}_1=\mathscr{M}_1(P)$时,$[AB]_P/\mathrm{sgn}[AB]_P$ 也过 $\mathscr{M}_1$. 于是

$$\prod_{B\in\mathscr{M}_1}B=\prod_{B\in\mathscr{M}_1}\frac{[AB]_P}{\mathrm{sgn}[AB]_P}\equiv\Big(\prod_{B\in\mathscr{M}_1}\mathrm{sgn}[AB]_P\Big)^{-1}\cdot\prod_{B\in\mathscr{M}_1}(AB)$$

$$\equiv A^{\frac{|P|-1}{q-1}}\Big(\prod_{B\in\mathscr{M}_1}\mathrm{sgn}[AB]_P\Big)^{-1}\Big(\prod_{B\in\mathscr{M}_1}B\Big)\pmod P.$$

由 $P \nmid \prod_{B\in\mathscr{M}_1} B$ 可知

$$\left\{\frac{A}{P}\right\} \equiv A^{\frac{|P|-1}{q-1}} \equiv \prod_{B\in\mathscr{M}_1} \mathrm{sgn}[AB]_P \pmod{P}.$$

由于同余式两端都是 $\boldsymbol{F}_q^*$ 中的元素，所以必然相等. 证毕. ▌

现在着手证高次互反律. 设首1不可约多项式 P 和 Q 的次数分别为 s 和 t，且 $s\geqslant t$. 用 P 去除 AQ，得到

$$AQ = BP + [AQ]_P = f(A)P + g(A). \qquad (6.1.1)$$

于是有两个 $\boldsymbol{F}_q$-线性映射：

$$f: \mathscr{M}(P) \cup \{0\} = \{A \in \boldsymbol{F}_q[T]: \deg A < s\}$$
$$\to \{B \in \boldsymbol{F}_q[T]: \deg B < t\};$$
$$g: \mathscr{M}(P) \cup \{0\} \to \mathscr{M}(P) \cup \{0\}.$$

其中 $f(A)=B, g(A)=[AQ]_P$. 而 g 为 $\boldsymbol{F}_q$-向量空间 $\mathscr{M}(P)\cup\{0\}$ 的自同构，f 为满同态，并且

$$\mathrm{Ker}(f) = \{A \in \boldsymbol{F}_q[T]: \deg A < s - t\}.$$

由引理6.1.1可知

$$\left\{\frac{Q}{P}\right\} = \prod_{A\in\mathscr{M}_1(P)} \mathrm{sgn}(g(A)). \qquad (6.1.2)$$

如果 $\deg A < s-t$，则

$$f(A) = 0,\ g(A) = AQ,\ \mathrm{sgn}(g(A)) = 1.$$

以下设 $A\in\mathscr{M}_1(P)$，并且 $s-t\leqslant\deg A\leqslant s-1$. 这样 A 的总数为

$$q^{s-1} + q^{s-2} + \cdots + q^{s-t} = q^{s-t}(q^t - 1)/(q - 1).$$

不难看出，对这样的 A，有 $f(A)\in\mathscr{M}_1(Q)$，并且

$$f: \{A \in \mathscr{M}_0(P): s - t \leqslant \deg A \leqslant s - 1\} \to \mathscr{M}_1(Q)$$

是 q^{s-t} 对1的映射.

类似地，对每个 $B'\in\boldsymbol{F}_q[T]$，用 Q 去除 $B'P$，得到

$$B'P = A'Q + [B'P]_Q = f'(B')Q + g'(B'). \quad (6.1.3)$$

其中 f' 和 g' 是 $\boldsymbol{F}_q$-线性映射，

$$f'(\mathscr{M}_1(Q)) \subseteq \{A' \in \mathscr{M}_1(P): s - t \leqslant \deg A' \leqslant s - 1\},$$

并且

$$\left\{\frac{P}{Q}\right\} = \sum_{B' \in \mathscr{M}_1(Q)} \operatorname{sgn}(g'(B')). \tag{6.1.4}$$

现在我们固定一个 $A_0 \in \mathscr{M}_1(Q)$，用 Q 去除 B_0P，得

$$B_0P = A_0Q + R_0. \tag{6.1.5}$$

其中 $\deg R_0 \leqslant t-1$，$A_0 \in \mathscr{M}_1(P)$，$s-t \leqslant \deg A_0 \leqslant s-1$. 而用 P 去除 A_0Q，则为

$$A_0Q = B_0P + (-R_0),$$

并且对每个

$$\begin{aligned} A_0 + C \in f^{-1}(B_0) &= A_0 + \operatorname{Ker} f \\ &= A_0 + \{C \in \boldsymbol{F}_q[T] : \deg C < s - t\} \end{aligned}$$

均有

$$(A_0 + C)Q = B_0P + (CQ - R_0). \tag{6.1.6}$$

于是有

$$\begin{aligned} \left\{\frac{P}{Q}\right\}^{-1} \cdot \left\{\frac{Q}{P}\right\} &= \prod_{\substack{A \in \mathscr{M}_1(P) \\ s-t \leqslant \deg A \leqslant s-1}} \operatorname{sgn}(g(A)) \cdot \prod_{B \in \mathscr{M}_1(Q)} \operatorname{sgn}(g'(B))^{-1} \\ &= \prod_{B_0 \in \mathscr{M}_1(Q)} \Big(\operatorname{sgn}(R_0)^{-1} \cdot \prod_{\substack{A \in \mathscr{M}_1(P) \\ f(A) = B_0}} \operatorname{sgn}(g(A)) \Big). \end{aligned}$$

但是

$$\begin{aligned} &\operatorname{sgn}(R_0)^{-1} \cdot \prod_{\substack{A \in \mathscr{M}_1(P) \\ f(A) = B_0}} \operatorname{sgn}(g(A)) \\ &= \operatorname{sgn}(R_0)^{-1} \cdot \prod_{\deg C < s-t} \operatorname{sgn}(CQ - R_0) \\ &= \operatorname{sgn}(R_0)^{-1} \cdot \operatorname{sgn}(-R_0) \cdot \prod_{0 \leqslant \deg C < s-t} \operatorname{sgn}(CQ - R_0) \\ &= -\prod_{0 \leqslant \deg C < s-t} \operatorname{sgn}(C) \\ &= -\prod_{\lambda=0}^{s-t-1} \prod_{\substack{a_\lambda, \cdots, a_0 \in \boldsymbol{F}_q \\ a_\lambda \neq 0}} \operatorname{sgn}(a_\lambda T^\lambda + a_{\lambda-1} T^{\lambda-1} + \cdots + a_0) \\ &= -\prod_{\lambda=0}^{s-t-1} \Big(\prod_{a_\lambda \in \boldsymbol{F}_q^*} a_\lambda \Big)^{q^\lambda} = -\prod_{\lambda=0}^{s-t-1} (-1) = (-1)^{s-t-1}. \end{aligned}$$

于是有

$$\left\{\frac{P}{Q}\right\}\cdot\left\{\frac{Q}{P}\right\}^{-1}=\prod_{B_0\in\mathscr{A}_1(Q)}(-1)^{s-t-1}=(-1)^{(s-t-1)\frac{|Q|-1}{q-1}}$$

$$=(-1)^{(s-t-1)t}=(-1)^{st}.$$

这就证明了高次互反律.

第二个证明(用指数函数)　Serre 在文献[51]中给出古典二次互反律的一个证明,其方法是利用正弦函数的一个恒等式,并且说这个证明是 Eisenstein 于1845年得到的. 现在我们仿照这个方法,用第4.4节中的 Goss 指数函数

$$e(z)=z\prod_{0\neq\alpha\in L}\left(1-\frac{z}{\alpha}\right)\tag{6.1.7}$$

来证明 $R=\boldsymbol{F}_q[T]$上的高次互反律,这里 $L=\tilde{\pi}R$,而 $\tilde{\pi}$ 是由 § 4.4 给出的 k_∞^{ac} 中的元素. 我们在注记4.4.5中曾经指出,$e(z)$可看成是 $\sin x$ 的模拟.

在定理4.4.4中曾表明 $e(Tz)=Te(z)+e(z)^q$. 所以若将 k_∞^{ac} 赋以 Carlitz R-模结构,即 T 在 $\alpha\in k_\infty^{ac}$上的作用为

$$\rho_T(\alpha)=\alpha^T=T\alpha+\alpha^q,$$

而对每个 $M\in R$,有

$$\rho_M(\alpha)=\alpha^M=\sum_{i=0}^{d}\begin{bmatrix}M\\ i\end{bmatrix}\alpha^{q^i},$$

其中 $d=\deg M$, $\begin{bmatrix}M\\ i\end{bmatrix}\in R$, $\begin{bmatrix}M\\ 0\end{bmatrix}=M$, $\begin{bmatrix}M\\ d\end{bmatrix}=1$. 从而有

$$\rho_M(e(z))=e(Mz)\quad(M\in R).$$

引理6.1.2　对每个 $a\in R_1$,有

$$a\prod_{\substack{b\in a^{-1}L/L\\ b\neq 0}}e(b)^{-1}=1.$$

证明　基于恒等式

$$\rho_a(e(z))=e(az)=ae(z)\prod_{\substack{b\in a^{-1}L/L\\ b\neq 0}}\left(1-\frac{e(z)}{e(b)}\right),\tag{6.1.8}$$

由于 $|a^{-1}L/L|=|R/(a)|=q^{\deg a}$,可知上式两端均为 $w=e(z)$的

$q^{\deg a}$次多项式. 由于$e(z)$是以L为周期的函数,并且L是它的零点集合,所以上式两端均有$q^{\deg a}$个不同的根$w=e(b)$($b\in a^{-1}L/L$). 因此它们至多相差一个常数. 进而,$\rho_a(e(z))=\begin{bmatrix}a\\1\end{bmatrix}e(z)+\cdots$,$\begin{bmatrix}a\\1\end{bmatrix}=a$. 所以将上式两端看作$w$的多项式时,$w$的一次项的系数均为$a$,因此上式为恒等式. 考察此恒等式关于$w=e(z)$的最高次($q^{\deg a}$次)项的系数,即得到本引理的证明. ▌

现在着手证明高次互反律. 由于函数$e(z)$的周期为$L=\tilde{\pi}R$,所以对每个$A\in R$,有

$$e\left(\frac{QA}{P}\tilde{\pi}\right)=\mathrm{sgn}([QA]_P)\cdot e\left(\frac{[QA]_P/\mathrm{sgn}[QA]_P}{P}\tilde{\pi}\right).$$

于是

$$\prod_{A\in\mathscr{A}_1(P)}e\left(\frac{QA}{P}\tilde{\pi}\right)=\prod_{A\in\mathscr{A}_1(P)}\mathrm{sgn}([QA]_P)\cdot\prod_{A\in\mathscr{A}_1(P)}e\left(\frac{A}{P}\tilde{\pi}\right).$$

由引理6.1.1可知

$$\left\{\frac{Q}{P}\right\}=\prod_{A\in\mathscr{A}_1(P)}e\left(\frac{QA}{P}\tilde{\pi}\right)\Big/e\left(\frac{A}{P}\tilde{\pi}\right).$$

由(6.1.8)式知

$$\begin{aligned}e\left(\frac{QA}{P}\tilde{\pi}\right)&=Qe\left(\frac{A}{P}\tilde{\pi}\right)\prod_{\substack{b\in Q^{-1}L/L\\ b\neq 0}}\left(1-\frac{e\left(\frac{A}{P}\tilde{\pi}\right)}{e(b)}\right)\\&=Qe\left(\frac{A}{P}\tilde{\pi}\right)\prod_{B\in\mathscr{A}(Q)}\left(1-\frac{e\left(\frac{A}{P}\tilde{\pi}\right)}{e\left(\frac{B}{Q}\tilde{\pi}\right)}\right)\\&=Qe\left(\frac{A}{P}\tilde{\pi}\right)\prod_{B\in\mathscr{A}_1(Q)}\left(1-\left[\frac{e\left(\frac{A}{P}\tilde{\pi}\right)}{e\left(\frac{B}{Q}\tilde{\pi}\right)}\right]^{q-1}\right).\end{aligned}$$

所以

$$\left\{\frac{Q}{P}\right\}=\prod_{A\in\mathscr{M}_1(P)}\left[Q\prod_{B\in\mathscr{M}_1(Q)}\left(1-\left(\frac{e\left(\frac{A}{P}\tilde{\pi}\right)}{e\left(\frac{B}{Q}\tilde{\pi}\right)}\right)^{q-1}\right)\right]$$

$$=\prod_{A\in\mathscr{M}_1(P)}\left[Q\prod_{B\in\mathscr{M}_1(Q)}e\left(\frac{B}{Q}\tilde{\pi}\right)^{-(q-1)}\left(e\left(\frac{B}{Q}\tilde{\pi}\right)^{q-1}-e\left(\frac{A}{P}\tilde{\pi}\right)^{q-1}\right)\right].$$

利用引理6.1.2，得到

$$Q\prod_{B\in\mathscr{M}_1(Q)}e\left(\frac{B}{Q}\tilde{\pi}\right)^{-(q-1)}=(-1)^{\frac{|Q|-1}{q-1}}Q\prod_{B\in\mathscr{M}_1(Q)}e\left(\frac{B}{Q}\tilde{\pi}\right)^{-1}$$

$$=(-1)^{\frac{|Q|-1}{q-1}}Q\prod_{\substack{b\in Q^{-1}L/L\\ b\neq 0}}e(b)^{-1}=(-1)^{\frac{|Q|-1}{q-1}}.$$

所以

$$\left\{\frac{Q}{P}\right\}=(-1)^{\frac{|Q|-1}{q-1}\cdot\frac{|P|-1}{q-1}}\prod_{\substack{A\in\mathscr{M}_1(P)\\ B\in\mathscr{M}_1(Q)}}\left(e\left(\frac{B}{Q}\tilde{\pi}\right)^{q-1}-e\left(\frac{A}{P}\tilde{\pi}\right)^{q-1}\right).$$

类似地有

$$\left\{\frac{P}{Q}\right\}=(-1)^{\frac{|Q|-1}{q-1}\cdot\frac{|P|-1}{q-1}}\prod_{\substack{A\in\mathscr{M}_1(P)\\ B\in\mathscr{M}_1(Q)}}\left(e\left(\frac{A}{P}\tilde{\pi}\right)^{q-1}-e\left(\frac{B}{Q}\tilde{\pi}\right)^{q-1}\right).$$

因此

$$\left\{\frac{P}{Q}\right\}\cdot\left\{\frac{Q}{P}\right\}^{-1}=\prod_{\substack{A\in\mathscr{M}_1(P)\\ B\in\mathscr{M}_1(Q)}}(-1)=(-1)^{\frac{|P|-1}{q-1}\cdot\frac{|Q|-1}{q-1}}.$$

第三个证明(用 torsion 元素)　对每个 $M\in R_1$，像前面那样，我们用 Λ_M 表示 Carlitz R-模 k^{ac} 中的 M-torsion 子模，并以 λ_M 表示一个固定的本原 M-torsion 元素，则

$$\lambda_Q^{BP}=\lambda_Q^{[BP]_Q}=\mathrm{sgn}([BP]_Q)\cdot\lambda_Q^{[BP]_Q/\mathrm{sgn}([BP]_Q)}.$$

所以

$$\prod_{B\in\mathscr{M}_1(Q)}\lambda_Q^{BP}=\prod_{B\in\mathscr{M}_1(Q)}\mathrm{sgn}[BP]_Q\cdot\prod_{B\in\mathscr{M}_1(Q)}\lambda_Q^{B}.$$

由引理6.1.1表明

$$\left\{\frac{P}{Q}\right\}=\prod_{B\in\mathscr{A}_1(Q)}\lambda_Q^{BP}/\lambda_Q^B. \tag{6.1.9}$$

由于 λ_P 在 $k=\boldsymbol{F}_q[T]$ 上的极小多项式为

$$u^P/u=\prod_{0\neq u\in\Lambda_P}(u-\lambda)=\prod_{A\in\mathscr{A}(P)}(u-\lambda_P^A)$$

$$=\prod_{A\in\mathscr{A}_1(P)}(u^{q-1}-(\lambda_P^A)^{q-1}),$$

所以(6.1.9)式变为(令 $u=\lambda_Q^B$):

$$\left\{\frac{P}{Q}\right\}=\prod_{\substack{A\in\mathscr{A}_1(P)\\B\in\mathscr{A}_1(Q)}}((\lambda_Q^B)^{q-1}-(\lambda_P^A)^{q-1}).$$

同样有 $\left\{\frac{Q}{P}\right\}=\prod_{\substack{A\in\mathscr{A}_1(P)\\B\in\mathscr{A}_1(Q)}}((\lambda_P^A)^{q-1}-(\lambda_Q^B)^{q-1})$. 因此

$$\left\{\frac{P}{Q}\right\}\cdot\left\{\frac{Q}{P}\right\}^{-1}=\prod_{\substack{A\in\mathscr{A}_1(P)\\B\in\mathscr{A}_1(Q)}}(-1)=(-1)^{\frac{|P|-1}{q-1}\cdot\frac{|Q|-1}{q-1}}.$$

第四个证明(用高斯和)　熟知古典二次互反律可用二次高斯和

$$G_p(m)=\sum_{a=1}^{p-1}\left\{\frac{a}{p}\right\}\zeta_p^{am}=\prod_{k=1}^{\frac{p-1}{2}}(\zeta_p^{(2k-1)m}-\zeta_p^{-(2k-1)m})\in\boldsymbol{Q}(\zeta_p)$$

的性质推出来,其中 p 为奇素数, $p\nmid m$, $\zeta_p=e^{\frac{2\pi i}{p}}$. 现在我们在分圆函数域中构作类似的高斯和,用以证明高次互反律.

对每个 $M\in R=\boldsymbol{F}_q[T]$, $P\nmid M$,定义

$$G_P(M)=\prod_{A\in\mathscr{A}_1(P)}\lambda_P^{AM}\in k(\Lambda_P)\quad(k=\boldsymbol{F}_q(T)).$$

以下的引理表明这种高斯和具有与古典高斯和相似的性质.

引理6.1.3　设 P 和 Q 是 $\boldsymbol{F}_q[T]$ 中不同的首1不可约多项式, $M\in\boldsymbol{F}_q[T]$, $P\nmid M$,则有:

(1) $G_P(M)=\left\{\frac{M}{P}\right\}G_P(1)$;

(2) $G_P(1)^{q-1}=P^*$,其中 $P^*=\left\{\frac{-1}{P}\right\}P$;

(3) $G_P(1)^{|Q|}\equiv\left\{\frac{Q}{P}\right\}G_P(1)\pmod{Q}$.

证明 (1) 简记 $\mathscr{M}=\mathscr{M}(P)$, $\mathscr{M}_1=\mathscr{M}_1(P)$, 则

$$G_P(M)=\prod_{A\in\mathscr{M}_1}\lambda_P^{[AM]_P}=\prod_{A\in\mathscr{M}_1}\operatorname{sgn}[AM]_P\cdot\prod_{A\in\mathscr{M}_1}\lambda_P^{[AM]_P/\operatorname{sgn}[AM]_P}$$

$$=\left\{\frac{M}{P}\right\}\prod_{A\in\mathscr{M}_1}\lambda_P^A\quad(\text{由引理 6.1.1})$$

$$=\left\{\frac{M}{P}\right\}G_P(1).$$

(2) 由于

$$\prod_{A\in\mathscr{M}}(u-\lambda_P^A)=u^P/u=\sum_{i=0}^{s}\begin{bmatrix}P\\i\end{bmatrix}u^{q^i-1}\quad(s=\deg P),$$

令 $u=0$,得到

$$\prod_{A\in\mathscr{M}}(-\lambda_P^A)=\begin{bmatrix}P\\0\end{bmatrix}=P,$$

但是

$$\prod_{A\in\mathscr{M}}\lambda_P^A=\Big(\prod_{A\in\mathscr{M}_1}\lambda_P^A\Big)^{q-1}\Big(\prod_{a\in F_q^\times}a\Big)^{|\mathscr{M}_1|}=(-1)^{\frac{|P|-1}{q-1}}G_P(1)^{q-1}$$

$$=\left\{\frac{-1}{P}\right\}G_P(1)^{q-1}.$$

因此 $G_P(1)^{q-1}=P^*$.

(3) 我们知道 $u^Q=\sum_{i=0}^{t}\begin{bmatrix}Q\\i\end{bmatrix}u^{q^i}$ $(t=\deg Q)$的系数$\begin{bmatrix}Q\\i\end{bmatrix}$ $(0\leqslant i\leqslant t-1)$均被 Q 整除. 因此 $u^Q\equiv u^{|Q|}\pmod{Q}$. 于是

$$G_P(1)^{|Q|}=\Big(\prod_{A\in\mathscr{M}_1}\lambda_P^A\Big)^{|Q|}\equiv\prod_{A\in\mathscr{M}_1}\lambda_P^{AQ}$$

$$=\left\{\frac{Q}{P}\right\}G_P(1)\pmod{Q}.$$ 这就证明了引理 6.1.3. ▌

现在证高次互反律:由于

$$G_P(1)^{|Q|}=(G_P(1)^{q-1})^{\frac{|Q|-1}{q-1}}G_P(1)$$

$$=(P^*)^{\frac{|Q|-1}{q-1}}G_P(1)\quad(\text{由引理 6.1.3.(2)})$$

$$\equiv \left\{\frac{-1}{P}\right\}^{\frac{|Q|-1}{q-1}}\left\{\frac{P}{Q}\right\}G_P(1)\pmod Q$$

$$\equiv (-1)^{\frac{|P|-1}{q-1}\cdot\frac{|Q|-1}{q-1}}\left\{\frac{P}{Q}\right\}G_P(1)\pmod Q.$$

再由引理6.1.3的(3)可知

$$\left\{\frac{P}{Q}\right\}G_P(1)\equiv(-1)^{\frac{|P|-1}{q-1}\cdot\frac{|Q|-1}{q-1}}\left\{\frac{P}{Q}\right\}G_P(1)\pmod Q.$$

由于 $G_P(1)^{q-1}=\left\{\frac{-1}{P}\right\}P$ 与 Q 互素，所以上式两端可去掉 $G_P(1)$，即得高次互反律.

第五个证明(用分圆函数域)　我们令 $k=\boldsymbol{F}_q(T)$，$R=\boldsymbol{F}_q[T]$，$K=k(\Lambda_P)=k(\lambda_P)$，其中 λ_P 是一个固定的本原 P-torsion 元素. $G_P(1)$是由上节定义的高斯和，则 $G_P(1)\in K$. 熟知古典二次互反律$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$可以用 $\boldsymbol{Q}(\zeta_p)$的二次子域 $\boldsymbol{Q}(\sqrt{p^*})$ $\left(p^*=\left(\frac{-1}{p}\right)p\right)$来证明. 现在我们用 K 的子域 $L=k(G_P(1))$来证明高次互反律.

引理6.1.4　(1) L 是 K 的唯一的子域满足$[L:k]=q-1$，并且伽罗华群 $\mathrm{Gal}(L/k)=\{\tau_a:a\in\boldsymbol{F}_q^*\}$，其中 $\tau_a(G_P(1))=aG_P(1)$.

(2) R 中每个首1不可约多项式 Q $(Q\neq P)$在 L 中不分歧，并且关于 Q 的 Frobenius 自同构为$\left[\frac{L/K}{Q}\right]=\tau_a$，其中 $a=\left\{\frac{P^*}{Q}\right\}$.

证明　由引理6.1.3知，$G_P(1)$是多项式 $f(x)=x^{q-1}-P^*$ 的根. 而 $f(x)$是关于 P 的 Eisenstein 多项式，即它在 k 上是不可约的. 所以$[L:k]=\deg f=q-1$，并且 $G_P(1)$的全部 k-共轭元素为 $aG_P(1)$ $(a\in\boldsymbol{F}_q^*)$. 由此即得伽罗华群 $\mathrm{Gal}(L/k)$. 最后，$\mathrm{Gal}(K/k)\cong(R/(P))^*$ 只有唯一的 $q-1$阶商群(因为$(R/(P))^*$是 $\Phi(P)=q^{\deg P}-1$阶循环群)，所以 L 是 K 的唯一子域满足$[L:k]=q-1$.

(2) Q 在 K 中不分歧(由定理1.2.1)，所以 Q 在 L 中也不分歧. 以 $\mathscr{P}$ 表示 Q 到 L 的一个扩充素理想. 则

$$\left[\frac{L/k}{Q}\right](G_P(1))\equiv G_P(1)^{|Q|}\pmod{\mathscr{P}}\quad\left(\text{由}\left[\frac{L/k}{Q}\right]\text{的定义}\right)$$

$$\equiv (P^*)^{\frac{|Q|-1}{q-1}} G_P(1) \quad (\text{因为 } G_P(1)^{q-1} = P^*)$$

$$\equiv \left\{\frac{P^*}{Q}\right\} G_P(1) \pmod{\mathscr{P}} \quad (\text{因为 } \mathscr{P} | Q).$$

由此即知$\left[\frac{L/k}{Q}\right]=\tau_a$，其中 $a=\left\{\frac{P^*}{Q}\right\}$. 证毕. ▌

现在证高次互反律：由引理6.1.4可知

$$\left[\frac{L/k}{Q}\right]=\tau_a,$$

其中

$$a = \left\{\frac{P^*}{Q}\right\} = \left\{\frac{-1}{Q}\right\}^{\frac{|P|-1}{q-1}} \cdot \left\{\frac{P}{Q}\right\}$$

$$= (-1)^{\frac{|P|-1}{q-1} \cdot \frac{|Q|-1}{q-1}} \cdot \left\{\frac{P}{Q}\right\}.$$

另一方面，Q 在 K 中的 Frobenius 自同构为$\left[\frac{K/k}{Q}\right]=\sigma_Q$，其中 $\sigma_Q(\lambda_P)=\lambda_P^Q$. 而 σ_Q 在 L 上的限制为 τ_a，所以

$$aG_P(1)=\tau_a(G_P(1)) = \sigma_Q(G_P(1)) = \sigma_Q\Big(\prod_{A \in \mathscr{M}_1(P)} \lambda_P^A\Big)$$

$$= \prod_{A \in \mathscr{M}_1(P)} \lambda_P^{AQ} = G_P(Q) = \left\{\frac{Q}{P}\right\} G_P(1).$$

这就证得了高次互反律$\left\{\frac{Q}{P}\right\}=(-1)^{\frac{|Q|-1}{q-1}\cdot\frac{|P|-1}{q-1}} \cdot \left\{\frac{P}{Q}\right\}$. ▌

§6.2 正 规 整 基

设 p 是奇素数，$\zeta_p=e^{\frac{2\pi i}{p}}$，则$\{\zeta_p^i : 1 \leqslant i \leqslant p-1\}$是分圆数域 $K=Q(\zeta_p)$的一组整基，并且这是一组正规整基，即整基中 $p-1$个元素是彼此共轭的. 对于 K 的任何子域 L，$N_{K/L}(\zeta_p)$的所有共轭元素构成 L 的一组正规整基. 设 M 和 N 是 Q 的有限 Galois 扩张，并且它们是线性无缘的，即 $M \cap N=Q$. 如果 M 和 N 分别有正规整基$\{\alpha_1, \cdots, \alpha_m\}$和$\{\beta_1, \cdots, \beta_n\}$，$m=[M:Q]$，$n=[N:Q]$，则易知$\{\alpha_i\beta_j : 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$为 MN 的正规整基. 于是，若 m 是一些不同奇素数的乘积，则 $K=Q(\zeta_m)$和它的子域 L 均有正规整基，而且

$N_{K/L}(\zeta_m)$的全部共轭元素形成域 L 的正规整基.

现在设 P 是 $R=\boldsymbol{F}_q[T]$中首1不可约多项式,则分圆函数域 $K=k(\Lambda_P)$的整数环为 $R[\lambda_P]$. 于是$\{\lambda_P^i:1\leqslant i\leqslant\Phi(P)-1\}$是 K 的一组整基(即 R-模 O_K 的一组基). 但这不是正规整基,从而由它不能自然地给出 K 的每个子域的(正规)整基. 现在我们介绍 Chapman[6]给出的 $K=k(\Lambda_P)$的一组正规整基. 先考虑 $\deg P=1$的情形.

定理6.2.1　设 $P=T-w$, $w\in\boldsymbol{F}_q$. 令 $k=\boldsymbol{F}_q(T)$, $K=k(\Lambda_P)$, $u=(w-T)^{\frac{1}{q-1}}$,则 $\eta=(1-u^{q-1})/(1-u)\in O_K$,并且 η 的所有 k-共轭元素形成 O_K 的一组正规整基.

证明　由于 λ_P 在 k 上的极小多项式为 $x^P/x=x^T/x-w=T-w+x^{q-1}$,所以 u 是本原 P-torsion 元素,而 K/k 的伽罗华群为 $\{\sigma_a:a\in\boldsymbol{F}_q^*\}$,其中 $\sigma_a(u)=au$. 而 $O_K=R[u]$,即$\{1,u,\cdots,u^{q-2}\}$是 O_K的一组整基. 另一方面,对于每个 $a\in\boldsymbol{F}_q^*$,有

$$\sigma_a(\eta)=(1-u^{q-1})/(1-au),$$

从而

$$\sum_{a\in\boldsymbol{F}_q^*}a^{-j}\sigma_a(\eta)=\sum_{a\in\boldsymbol{F}_q^*}\sum_{i=0}^{q-2}a^{-j}(au)^i=\sum_{i=0}^{q-2}u^i\sum_{a\in\boldsymbol{F}_q^*}a^{i-j}$$
$$=-u^j\quad(0\leqslant j\leqslant q-2).$$

这就表明 η 的所有 k-共轭元素形成 O_K 的一组正规整基.　▌

以下设 $d=\deg P\geqslant 2$. 令 $k'=\boldsymbol{F}_{q^d}(T)$,则 $P(T)$在 $\boldsymbol{F}_{q^d}[T]$中完全分解成

$$P(T)=\prod_{i=0}^{d-1}(T-w_i)$$

其中 $w_i\in\boldsymbol{F}_{q^d}$, $w_{i+1}=w_i^q$.

记 $u_i=(w_i-T)^{\frac{1}{q^d-1}}$, $K_i'=k'(u_i)$, $K_P'=k'(u_1,\cdots,u_d)$.

引理6.2.2　$K=k(\Lambda_P)$是 K_P' 的子域.

证明　由于$\prod_{i=0}^{d-1}(w_i-T)^{a_i}$ $(0\leqslant a_i\leqslant q^d-1)$中只有当 $a_0=a_1=\cdots=a_{d-1}=0$时才是 k' 中元素的 q^d-1次幂,所以 K_P'/k'是$(q^d-1)^d$

次 Kummer 扩张，它的伽罗华群为

$$\mathrm{Gal}(K'_P/k') = \{(\tau_{\alpha_1}^{(1)}, \cdots, \tau_{\alpha_d}^{(d)}) : \alpha_i \in \boldsymbol{F}_q^*\},$$

其中对于 $\alpha \in \boldsymbol{F}_q^*$，有

$$\tau_\alpha^{(i)}(u_j) = \begin{cases} \alpha u_i, & \text{若 } j = i; \\ u_j, & \text{若 } j \neq i. \end{cases}$$

而 $\left\{\prod_{i=0}^{d-1} u_i^{a_i} : 0 \leqslant a_i < q^d - 1\right\}$ 是 K'_P 的一组 k'-基.

令

$$\delta_i = \prod_{j=0}^{d-1} u_{i+j}^{q^{d-1-j}} \quad (0 \leqslant i \leqslant d-1),$$

则

$$\delta_i^q = \prod_{j=0}^{d-1} u_{i+j}^{q^{d-j}} = u_i^{q^d-1} \prod_{j=0}^{d-1} u_{i+j+1}^{q^{d-1-j}} = (w_i - T)\delta_{i+1}.$$

令 $v_\alpha = \sum_{j=0}^{d-1} \alpha^{q^j} \delta_j \quad (\alpha \in \boldsymbol{F}_{q^d})$，则映射

$$\boldsymbol{F}_{q^d} \to K'_P, \quad \alpha \mapsto v_\alpha \tag{6.2.1}$$

是 $\boldsymbol{F}_q$-线性的. 由于

$$\begin{aligned} v_\alpha^q &= \sum_{i=0}^{d-1} \alpha^{q^{i+1}} \delta_i^q \\ &= \sum_{i=0}^{d-1} \alpha^{q^{i+1}} \delta_{i+1}(w_i - T) \\ &= \sum_{i=0}^{d-1} \alpha^{q^i} \delta_i (w_{i-1} - T), \end{aligned}$$

所以 T 在 v_α 上的 Carlitz 作用为

$$v_\alpha^T = v_\alpha^q + TV_\alpha = \sum_{i=0}^{d-1} \alpha^{q^i} \delta_i w_{i-1} = \sum_{i=0}^{d-1} (\alpha w)^{q^i} \delta_i = v_{\alpha w},$$

其中 $w = w_{-1} \in \boldsymbol{F}_{q^d}$. 所以对每个 $r \geqslant 0$，$v_\alpha^{T^r} = v_{\alpha w^r}$. 再由映射(6.2.1)是 $\boldsymbol{F}_q$-线性的，可知对每个 $f(T) \in \boldsymbol{F}_q[T]$ 和 $\alpha \in \boldsymbol{F}_{q^d}$，有 $v_\alpha^{f(T)} = v_{\alpha f(w)}$. 特别地，$v_\alpha^P = v_{\alpha P(w)} = v_0 = 0$，即对每个 $\alpha \in \boldsymbol{F}_{q^d}$，$v_\alpha \in \Lambda_P$. 由于 $\left\{\prod_{i=0}^{d-1} u_i^{a_i} : 0 \leqslant a_i < q^d - 1\right\}$ 是 K'_P 的 k'-基，可知 $v_1 \neq 0$，即 v_1 为本原 P-torsion 元素. 这就表明 $\Lambda_P \subseteq K'_P$，即 $K \subseteq K'_P$. ▌

于是我们有域的扩张图表如图6.1所示.

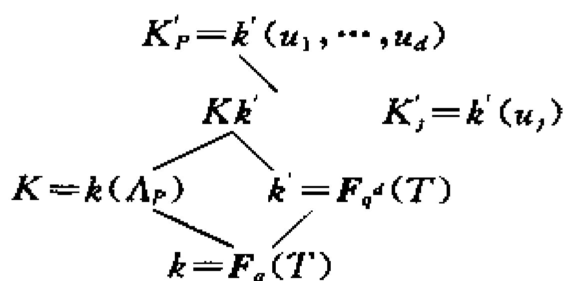


图　6.1

现在计算这些扩张的伽罗华群. 易知 Gal (k'/k) 是由 Frobenius 自同构 σ 生成的 d 阶循环群. 这里对每个 $a=\sum a_i T^i \in F_{q^d}[T]$, $\sigma(a)=\sum a_i^q T^i$. 于是 $\sigma(w_i-T)=w_{i+1}-T$. σ 可扩充成 $\mathrm{Gal}(K'_P/k)$ 中元素 ϕ, 使得 $\phi(u_i)=u_{i+1}$ $(0\leqslant i\leqslant d-1)$. 于是 ϕ 的阶为 d. 我们在引理6.2.2的证明中已算出

$$G=\mathrm{Gal}(K'_P/k')$$
$$=\{\tau_\alpha=(\tau^{(1)}_{\alpha_1},\cdots,\tau^{(d)}_{\alpha_d});\alpha=(\alpha_1,\cdots,\alpha_d)\in(F^*_{q^d})^d\}.$$

对于每个 $0\leqslant j\leqslant d-1$, 有

$$\tau_\alpha\phi^j(u_i)=\tau_\alpha(u_{i+j})=\alpha_{i+j}u_{i+j}.$$

所以 $\tau_\alpha\phi^j=\tau_{\alpha'}\phi^{j'}\Leftrightarrow j\equiv j' \pmod{d}$ 并且 $\alpha=\alpha'$. 这就表明了 K'_P/k 是伽罗华扩张, 并且

$$\Gamma=\mathrm{Gal}(K'_P/k)=\{\tau_\alpha\phi^j;\alpha\in(F^*_{q^d})^d,0\leqslant j\leqslant d-1\}.$$

由于

$$\phi\tau_\alpha\phi^{-1}(u_i)=\phi\tau_\alpha(u_{i-1})=\phi(\alpha_{i-1}u_{i-1})=\alpha^q_{i-1}u_i,$$

可知 $\phi\tau_\alpha\phi^{-1}=\tau_{\alpha^\phi}$, 其中对 $\alpha=(\alpha_1,\cdots,\alpha_d)$ 定义 $\alpha^\phi=(\alpha^q_d,\alpha^q_1,\cdots,\alpha^q_{d-1})$. 于是 Γ 为 $\langle\phi\rangle$ 和 G 的半直积.

Γ 在 δ_i 上的作用为

$$\phi(\delta_i)=\prod_{j=0}^{d-1}\phi(u_{i+j})^{q^{d-1-j}}=\prod_{j=0}^{d-1}u_{i+j+1}^{q^{d-1-j}}=\delta_{i+1},$$

$$\tau_\alpha(\delta_i)=\prod_{j=0}^{d-1}(\alpha_{i+j}u_{i+j})^{q^{d-1-j}}=\delta_i\hat{\alpha}_i,$$

其中 $\hat{\alpha}_i=\prod_{j=0}^{d-1}\alpha_{i+j}^{q^{d-1-j}}$. 于是对每个 $\beta\in F_{q^d}$, 有

$$\phi(v_\beta)=\sum_{i=0}^{d-1}\phi(\beta^{q^i}\delta_i)=\sum_{i=0}^{d-1}\beta^{q^{i+1}}\delta_{i+1}=v_\beta.$$

$$\tau_\alpha(v_\beta)=\sum_{i=0}^{d-1}\beta^{q^i}\hat{\alpha}_i\delta_i=\sum_{i=0}^{d-1}(\hat{\alpha}_0\beta)^{q^i}\delta_i=v_{\hat{\alpha}_0\beta}.$$

这就表明

$$\mathrm{Gal}(K'_P/K)=\{\tau_\alpha\phi^j:0\leqslant j\leqslant d,\hat{\alpha}_0=\prod_{j=0}^{d-1}\alpha_i^{q^{d-1-j}}=1\},$$

$$\mathrm{Gal}(K'_P/Kk')=\{\tau_\alpha:\alpha=(\alpha_0,\cdots,\alpha_{d-1})\in(F_{q^d}^*)^d.\hat{\alpha}_0=1\},$$

令 $T_{L/K}$表示扩张 L/K 的迹函数. 现在可给出 $K=k(\Lambda_P)$的正规整基.

定理6.2.3 设 $d=\deg P\geqslant 2$，$P=P(T)$在 F_{q^d}中的 d 个根为 w_i $(0\leqslant i\leqslant d-1)$，$w_i^q=w_{i+1}$. 又令

$$u_i=(w_i-T)^{\frac{1}{q-1}}(0\leqslant i\leqslant d-1),\eta_j=(1-u_j^{q^d-1})/(1-u_j),$$

$$\eta'=\prod_{j=0}^{d-1}\eta_j,\quad \eta_P=(-1)^{d-1}T_{K'_p/Kk'}(\eta'),$$

则 $\eta_P\in K$,并且 η_P 的全部 k-共轭元素给出 K 的一组正规整基.

证明 记 $G_j=\mathrm{Gal}(K'_j/k')$. 由定理6.2.1可知 $O_{K'_j}=O_{k'}[G_j]\eta_j$ $(1\leqslant j\leqslant d)$. 由于 $G=\mathrm{Gal}(K'_P/k')$是 G_j $(1\leqslant j\leqslant d)$的直积,所以 η' 给出 K'_P/k'的正规整基,即 $O_{K'_p}=O_{k'}[G]\eta'$. 由于$[K'_P:k'K]=(q^d-1)^{d-1}$与 F_q 的特征互素,可知 $T_{K'_p/k'K}O_{K'_p}=O_{k'K}$. 因此通过 $T_{K'_p/k'K}$的作用,得到

$$O_{Kk'}=O_{k'}[\Delta]\eta_P,\qquad(6.2.2)$$

其中 $\Delta=\mathrm{Gal}(Kk'/k')\cong\mathrm{Gal}(K/k)$. 我们现在更明确地计算出 η_P,以表明 $\eta_P\in K$. 由定义知

$$(-1)^{d-1}\eta_P=\sum_{\tau\in\Sigma}\tau\left(\prod_{j=0}^{d-1}\sum_{i=0}^{q^d-2}u_j^i\right),$$

其中 $\Sigma=\mathrm{Gal}(K'_P/Kk')=\{\tau_\alpha:\alpha=(\alpha_0,\cdots,\alpha_{d-1})\in(F_{q^d}^*)^d,\hat{\alpha}_0=\prod_{j=0}^{d-1}\alpha_j^{q^{d-1-j}}=1\}$. 因此

$$(-1)^{d-1}\eta_P=\sum_\alpha\left(\prod_{j=0}^{d-1}\sum_{i=0}^{q^d-2}\alpha_j^i u_j^i\right)$$

$$(\alpha\text{ 过}\{\alpha=(\alpha_0,\cdots,\alpha_{d-1});\hat{\alpha}_0=1\})$$

$$= \sum_{\alpha} \sum_{i \in X} \prod_{j=0}^{d-1} \alpha_j^{i_j} u_j^{i_j}$$

$$(i \text{ 过 } X = \{i = (i_0, \cdots, i_{d-1}) : 0 \leqslant i_j < q^d - 1\})$$

$$= \sum_{i \in X} \left(\sum_{\alpha} \prod_{j=0}^{d-1} \alpha_j^{i_j} \right) \prod_{j=0}^{d-1} u_j^{i_j}.$$

注意，Σ 是乘法群，而对每个 $i \in X$，映射

$$\psi_i : \Sigma \to \boldsymbol{F}_{q^d}^*, \psi_i(\alpha) = \prod_{j=0}^{d-1} \alpha_j^{i_j}$$

为群同态. 于是

$$\sum_{\alpha} \prod_{j=0}^{d-1} \alpha_j^{i_j} = \sum_{\alpha} \psi_i(\alpha) \neq 0 \Longleftrightarrow \psi_i(\alpha) = 1 \quad (\text{对每个 } \alpha \in \Sigma)$$

$$\Longleftrightarrow i_j \equiv i_{j+1}^q \pmod{q^d - 1} \quad (0 \leqslant j \leqslant d-1).$$

以 $\langle s \rangle$ 表示 s 模 $q^d - 1$ 的最小非负剩余，则

$$\eta_P = (-1)^{d-1} \sum_{i=0}^{q^d-2} \left(\sum_{\alpha} 1 \right) \prod_{j=0}^{d-1} u_j^{\langle iq^{d-j-1} \rangle}$$

$$= \sum_{i=0}^{q^d-2} \prod_{j=0}^{d-1} u_j^{\langle iq^{d-j-1} \rangle} \in O_{Kk'}.$$

将 η_P 作用于 $\mathrm{Gal}(Kk'/K)$ 的生成元 ϕ，则

$$\phi(\eta_P) = \sum_{i=0}^{q^d-2} \prod_{j=0}^{d-1} u_{j+1}^{\langle iq^{d-j-1} \rangle} = \sum_{i=0}^{q^d-2} \prod_{j=0}^{d-1} u_j^{\langle iq^{d-j-1} \rangle} = \eta_P.$$

这就表明 $\eta_P \in O_K$. 最后将(6.2.2)式两端限制在 O_K 上，便得到 $O_K = O_k[\Delta]\eta_P$. 这就表明 η_P 的全部 k-共轭元素给出 O_K 的一组正规整基. ▌

注记　设 $\Delta = \mathrm{Gal}(K/k)$，$K = k(\Lambda_P)$，$\chi : \Delta \to \boldsymbol{F}_{q^d}^*$ 是 χ 的特征(取值于 $\boldsymbol{F}_{q^d}^*$). 所有这种特征形成了 $q^d - 1$ 阶循环群 $\hat{\Delta}$，并且有生成元 ρ，其中将 Δ 看成 $(\boldsymbol{F}_q[T]/(P))^*$ 时，$\rho(T) = w_{-1} \in \boldsymbol{F}_{q^d}^*$.

对每个元素 $\xi \in K$，定义 ξ 对 $\chi \in \hat{\Delta}$ 的拉格朗日 resolvent 为

$$\langle \xi | \chi \rangle = \sum_{\sigma \in \Delta} \chi(\sigma) \sigma(\xi).$$

对于数域 $K = \boldsymbol{Q}(\zeta_p)$ 和 $\xi = \zeta_p$ 的情形这就是高斯和. 对于现在的情

形，当$0 \leqslant i \leqslant q^d - 1$时($d = \deg P$)，可以算出

$$\langle \eta_P \mid \rho^i \rangle = \sum_{\sigma \in \Delta} \rho^i(\sigma^{-1}) \sigma(\eta_P) = -\prod_{j=0}^{d-1} u_j^{\langle i q^{d-j-1} \rangle}.$$

而对于$0 \leqslant r \leqslant d-1$，$\langle \eta_P \mid \rho^{q^r} \rangle = -\delta_r$ 本质上就是§5.3所介绍的高斯和.

参考文献

[1] Carlitz L. On certain functions connected with polynomials in a Galois fields. Duke Math Jour. 1935, 1: 137~168

[2] Carlitz L. A class of polynomials, Trans Amer Math Soc, 1938, 43:168~182

[3] Carlitz L. A set of polynomials. Duke Math Jour. 1940, 6:486~504

[4] Carlitz L. An analogue of Bernoulli polynomials. Duke Math Jour. 1941, 8:405~412

[5] Carlitz L. Finite sums and interpolation formulas over GF[P^n, x]. Duke Math Jour. 1948, 15:1001~1012

[6] Chapman R J. Carlitz modules and normal integral bases. J. London Math Soc. 1991, 44:250~260

[7] Cheng L and Feng K. On independence of cyclotomic units in function fields. Sci Sinica. 1988, 31:601~609

[8] Deligne P and Husemoller D. Survey of Drinfeld modules, Current Trends in Arithmetical Algebraic Geometry. Ribet K editor, Contemporary Mathematics. Amer Math Soc., Providence. 1986, 67: 25~91

[9] Drinfeld V G Elliptic modules (russian). Math, USSR-Sb. 1974, 94:594~627

[10] Feng K. A note on irregular prime polynomials in cyclotomic function fields. Jour of Number Theory. 1986, 22:240~245

[11] Feng K. Class number "parity" for cyclic function fields. Proceedings of the Workshop (The Arithmetic of Function Fields). 1991, Goss D, Hayes D R and Rosen M I (Edited), Walter de Gruyter. 1992, 103~116

[12] Feng K. Zeta function, class number and cyclotomic units of cyclotomic function fields. Advanced Studies in Pure Math, Vol. 21 (Zeta Functions in Geometry). 1992, 141~152

[13] Feng K. An elementary criterion on parity of class number of cyclic number fields. Scientia Sinica. 1982, 25:1032~1041

[14] Feng K and Gao W. Bernoulli-Goss polynomials and the class number of cyclotomic function fields. Sci Sinica. 1989, 32:1257~1263

[15] Feng K and Xu F. The Euler system in cyclotomic function fields. to appear in Jour of Number Theory. 1995

[16] Feng K and Yin L. On maximal indepedent systems of cyclotomic units in cyclotomic function fields. Sci Sinica, 1991, 34:252~261

[17] Gekeler E U. Drinfeld Modular Curves. Lecture Notes in Math. vol. 1231, Springer-Verlag, 1986

[18] Gekeler E U. On power sums of polynomials over finite fields. Joun. of Number, Theory, 1988, 30: 11～26

[19] Gekeler E U. Some identities for Bernoulli-Carlitz numbers. Joun. of Number Theory, 1989, 33: 209～219

[20] Gekeler E U. On relguarly of small primes in function fields. Joun. of Number Theory, 1990, 34: 114～127

[21] Goss D. von Staudt for $F_q[T]$ Duke Math Jour. 1978, 5: 885～910

[22] Goss D. v-adic zeta functions, L-series and measure for function fields. Inv Math. 1979, 55: 107～119

[23] Goss D. The Algebraist's upper half-plane. Bull Amer Math Soc, 1980, 2: 391～415

[24] Goss D. Kummer and Herbrand criterion in the theory of function fields. Jour. Number Theory, 1982, 14: 156～184

[25] Goss D. On a new type of L-function for algebraic curves over finite fields. Pacific J. Math. 1983, 105: 143～181

[26] Goss D. The arithmetic of function fields 2: The 'cyclotomic' theory Jour of Algebra. 1983, 81: 107～149

[27] Goss D. Analogies between global fields. Conference Proceedings of the Canadian Mathematical Society. 1987, 7: 83～114

[28] Goss D. The Γ-function in the arithmetic of function fields. Duke Math Jour. 1988, 56: 163～191

[29] Goss D. Fourier series, measures and divided power series in the theory of function fields. K-Theory 1989, 2: 533～555

[30] Goss D. A formal Mellin transform in the arithmetic of function fields. Trans. Amer Math Soc. 1991, 327: 567～582

[31] Goss D. Harmonic analysis and the flow of a Drinfeld module. Jour of Algebra, 1992, 146: 219～241

[32] Gras G. Class d'ideaux des corps abeliens et nombres de Bernoulli generalisis. Ann. Inst. Fourier, 1977, 27: 1～66

[33] Gras G and Gras M-N. Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de Q de degré premier impair. Ann Inst Fourier, Grenoble. 1975, 25: 1～22.

[34] Greenberg R. On p-adic L-functions and cyclotomic fields Ⅰ. Nagoya Math Jour. 1977, 67: 139～158

[35] Galovich S and Rosen M. The class number of cyclotomic function fields. Jour of Number Theory, 1981, 13: 363～375

[36] Galovich S and Rosen M. Units and class groups in cyclotomic function fields Jour. of Number Theory, 1982, 14: 156～184

[37] Galovich S and Rosen M. Distributions on rational function fields. Math Ann. 1981, 256: 549～560.

[38] Goss D and Sinnott W. Class groups of function fields. Joun. of Number Theory, 1985, 52: 507～516

[39] Hayes D. Explicit class field theory for rational function fields. Trans Amer Math Soc. 1974, 189: 77～91

[40] Hayes D. Explicit class field theory in global function fields, G. C. Rota (ed.) Stuies in Algebra and Number Theory. New York, Academic Press, 1979. 173～217

[41] Hayes D. A brief introduction to Drinfeld modules. Proceedings of the Workshop (The Arithmetic of Functions Fields) (1990) Edited by D. Goss, D. R. Hayes and M. I. Rosen Walter de Gruyter. 1992. 1～32

[42] Koblitz N. p-adic Numbers, p-adic Analysis and zeta functions. Springer-Verlag, 1984.

[43] Kolyvagin V A. Euler systems, In Grothendieck Festschrift. vol. 2, Drog Math 1990, 87: 435～483

[44] Kummer E. Uber eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke. J. Reine Angew. Math. 1955, 50: 212～232

[45] Lang S. Cyclotomic Fields I and II. GTM 121, Springer-Verlag, 1990

[46] Lee H. Power sums of polynomials in a Galois fields. Duke Math Jour. 1943, 10: 277～292

[47] Mazur B and Wiles A. Class fields of abelian extensions of $\boldsymbol{Q}$. Inv. Math. 1984, 76: 179～330

[48] Okada S. Kummer's theory for function fields. Jour of Number Theory, 1991, 38: 212～215

[49] Rosen M. The Hilbert class field in function fields. Exposition Math. 1987, 365～378

[50] Rubin K. The main conjecture. Appendix to [45], 397～419

[51] Sinnott W. On the Stickelberger ideal and the circular units of a cyclotomic field. Annals of Math. 1978, 108: 107～134

[52] Shu L. cyclotomic type theorems over global function fields. Thesis at Brown Univ, 1992

[53] Thaine F. On the ideal class groups of real abelian number fields. Ann of Math. 1988,128:1~18

[54] Thakur D. Gamma functions for function fields and Drinfeld modules. Ann of Math. 1991,134:25~64

[55] Thakur D. Gauss sums for $F_q[T]$. Inv. Math. 1988,94:105~122.

[56] Thakur D. Zeta measure associated to $F_q[T]$. Jour of Number Theory, 1990, 35:1~17

[57] Washington L. C. Introduction to Cyclotomic Fields. Springer-Verlag,1982

[58] Weiss E. Algebraic Number Theory McGraw-Hill ,1963.

[59] Yu J. Transcendence and Drinfeld modules. Inv. Math. 1986,83,507~517

[60] Yu J. Transcendence and special zeta values in characteristic p. Ann. of Math. 1991,134:1~23

现代数学丛书


ISBN 7-5323-3949-1

9 787532 339495 >

定 价: 30.00元